ENGINEERING IN ADVANCED RESEARCHSCIENCE AND TECHNOLOGY

ISSN 2352-8648
Vol.03, Issue.01
June-2022
Pages: -353-364

SECURE AND COVERT COMMUNICATION USING STEGANOGRAPHY BY WAVELET TRANSFORM

[1]A. Charan Babu, [2]A. Saidulu, [3]T. Ravindra Babu, [4]K. Sai Kumar,[5]U. Ankamma Rao, [6]T. Kartheek Reddy,
[1,2,3,4,5,6] student of ECE dept., Kallam Haranadhareddy Institute of Technology, Guntur.
[7]Mr. U. Srinivas, Assistant professor of ECE dept., Kallam Haranadhareddy Institute ofTechnology, Guntur.

ABSTRACT:

This paper presents a hybrid image steganography along with cryptography algorithm based on LS (Logical & Statistical) encryption scheme and lift wavelet domain of digital images. Currently, cryptography data can be easily intercepted by an intruder during transmission. So it may be treated as ineffectual in terms of security. In such a scenario, the proposed algorithm provides secured transmission by using cryptography and steganography techniques. In this algorithm a new LS encryption scheme is implemented for converting secret message into ciphertext. It is being done by using several parameters like 'data indicator', 'count indicator', 'gray code' and novel 'data conversion' techniques. The 'gray code' and novel 'data conversion' techniques are used to recover the inherent information at the receiver and to improve the security of the secret data. Moreover, it reduces the ciphertext length compared to the length of original secret data. Hence this scheme improves the payload capacity and helps to improve the quality metrics like Number of Pixels Change in Rate (NPCR), Peak Signal to Noise Ratio (PSNR), and Correlation (CORR) in the stego image. Furthermore, steganography scheme provides an ability to tackle the various attacks like noise, rotational, histogram and visual attacks. It is also shown that how the original message is recovered back from stego image successfully.

KEYWORDS: Image steganography, Lift Wavelet Transform (LWT), image security, stego image, spatial domain, cryptography

I. INTRODUCTION

Nowadays, the interpersonal sharing of information is growing rapidly due to the usage of smartphones and internet. In this regard, transferring personal information securely from one to another is a big challenge. The security of transferring information is mainly disturbed by the hackers. In such situations, data hiding techniques are very helpful to keep the information secured from intruders. Three fundamental feasible techniques are available for data hiding which are watermarking, steganography andcryptography.

In watermarking, ownership information is embedded in source data. It is mainly used to protect ownership information. Cryptography transforms the information into "ciphertext". However, aforementioned techniques do not provide complete immunity from data breaches. Steganography hides the covert information which may be audio, image, text or video into cover medium. The cover medium can be text, audio, image or video. The combination of steganography and cryptography techniques provides a better security than the individual techniques.

In steganography, stego object can be obtained by using several techniques like Spatial domain techniques, Spread spectrum technique, Statistical technique, Transform domain technique, Distortion technique, Masking and Filtering technique etc.,. In spatial domain technique, the secret information is directly embedded into the cover object without any modifications. It is further classified into Least Significant Bit (LSB) and Random Pixel Embedding method (RPE). The advantage of spatial domain technique is increased payload capacity. However, the level of security is moderate.

In spread spectrum technique, information is embedded in noise sequence which generates scrambled data. The stego image is produced by embedding the scrambled data in the cover image. This makes the recovery of secret information at the receiver is difficult. The transform domain technique is used to generate the stego object by hiding the secret data in sub-bands of the cover object. This provides better security at the cost of the payload capacity.

The distortion technique modifies the cover object based on the secret data in order to obtain the stego object. Due to this, high amount of noise component is generated in the output. In masking and filtering technique, the secret information is placed in significant locations of the cover medium. In this, the target object is clearly visible hence it is used only for copy right purpose.

This paper presents a hybrid technique which combines image steganography and cryptography. The steganography scheme was achieved by using transform domain (LWT) along with spatial domain (RPE) technique. This combination overcomes the drawbacks of the individual techniques. Hence the proposed steganography method has the ability to tackle various attacks like noise, rotational, histogram and visual attacks. Furthermore, the novel cryptography scheme (LS encryption) helps to improve the payload capacity and quality metrics like NPCR, PSNR and CORR.

II. LIFT WAVELET TRANSFORM (LWT)

LWT is a technique introduced by "Wim Sweldens". In this, the lifting scheme treated as an alternative approach for performing the DWT operation on signal by using biorthogonal wavelets. With this scheme, we reduces the conventional computations of DWT up to 50% which means DWT requires the cost is 4*(R+S)+2. But LWT requires only 2*(R+S+2) [22]. Moreover, it also increases the speed up to two times than the DWT and calculates the wavelet coefficients without auxiliary memory. The block diagram of LWT scheme is shown in Fig 1.

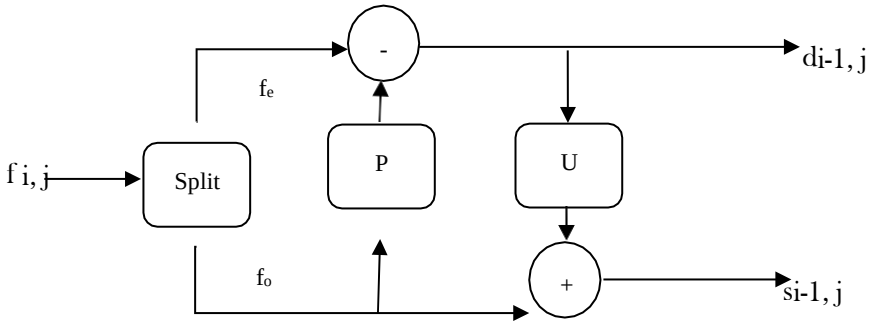


Fig 1. Block diagram of LWT

Initially, the source signal ($f_{i,j}$) is split into poly phase components i.e even (f_e) and odd (f_O) sets. In order to generate the detailed coefficients ($d_{i-1, j}$), the even sets of the source signal are subtracted with response of the predicted signal (P). To generate the smooth coefficients ($s_{i-1, j}$), we need to add the odd sets of source signal with the response of update signal (U). Such calculation of high ($s_{i-1, j}$) and low ($d_{i-1, j}$) frequency coefficients of input signal is termed as "Lifting Step". Furthermore for multi scale coefficients we need to apply the lifting step to the correspondent coefficient. The mathematical expressions of predicted function, updated function, detailed and smooth coefficients are as follows.

$$\text{Detailed coefficients } (d_{i-1, j}) = f_e - P(f_O) \quad (1)$$

$$\text{Smooth coefficients } (s_{i-1, j}) = f_O + U(d) \quad (2)$$

Where

$$\text{Prediction function of even samples } P(f_O) = (f_O + f_{O+2}) / 2 \quad (3)$$

$$\text{Updated function of details } U(d) = (d_{i-1} + d_i) / 4 \quad (4)$$

III. PROPOSED METHOD

Inspired from the cryptography and steganography techniques, a unique encryption algorithm (LS) along with steganography is proposed. The operation of proposed method is explained in two sections

1) Transmitter section.
2) Receiver section.

3.1 Transmitter Section

The block diagram of transmitter section is shown in Fig 2. The LS encryption algorithm is used as a first layer in transmitter section. It is used to encrypt the secret information to generate the ciphertext. The next layer performs steganography operation by concealed the ciphertext into cover object using LWT & RPE techniques.

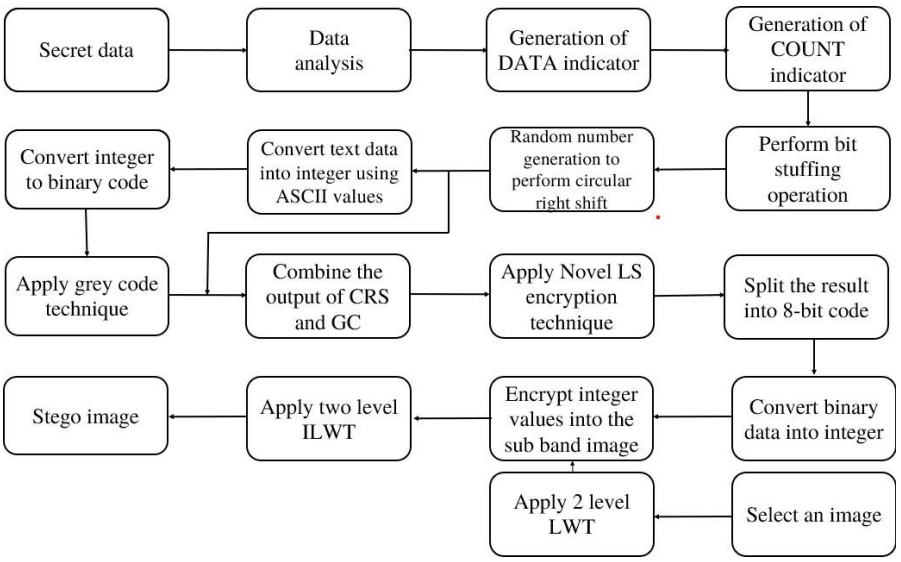


Fig 2. Block diagram of Transmitter Section

3.1.1 LS Encryption Algorithm

As shown in Fig 2. The LS encryption algorithm accepts secret data as an input and produces the ciphertext. It mainly involves three stages, they are 'Scrambled Parity Data' generation and 'Gray-code Data' generation and 'Ciphertext' generation.

- **Procedure for 'Scrambled Parity Data' Generation**

Secret Data: Generally the secret data can be available in three forms. They are 'alpha-numeric', 'numeric' and 'byte' data. Usually 'apha-numeric' data contains alphabets, numerical values and some special symbols ($, %, *, +, -, dot, /: and 'space'). Whereas 'numeric' data contains only numerical values (0 to 9). When coming to 'byte' data, it represents ISO define character set.

Step 1: In step 1, we assign 4-bit binary value to the correspondent data type and is called as 'data indicator'. The 'data indicator' of 'alpha-numeric' is represented as 1011. For 'numeric' data, it is represented as 1100 and for 'byte' data, it is represented as 1111. The purpose of 'data indicator' is used to identify data type at receiver.

If we take "HELLO WORLD" as an example for secret data then type of the data is 'alpha-numeric' and correspondent 'data indicator' (D) is 1011.

Step 2: In step 2, we count the number of characters in the secret data which is termed as 'count indicator'. It is represented in 10 bit binary form. The step 2 process will be helpful for retrieving the accurate secret data at receiver section.

In above example, the number of characters are 11. So 'Count Indicator' (C) is represented as

C = 0000001011 (11 in 10 bit-binary form) (5)

Step 3: The bits of the 'data indicator' is placed after every two bits in 'count indicator'. This is known as

'bit stuffing'. The resultant data produced after the 'bit stuffing' process is indicated as 'F'. The bit stuffing is used for retrieving the 'data indicator' and 'count indicator' from set of data in image at receiver section.

In this example, 'Data indicator' (D) is 1011 and 'Count indicator' (C) is 0000001011. Now each bit of the 'data indicator' is placed after every two bits in 'count indicator'. Then resultant data is shown in below and it is denoted as 'F'.

$$\therefore \quad F = 001000001110111 \tag{6}$$

Step 4: Next our aim is to generate the 'scrambled parity data' for the step 4 output. This can be done by performing the Circular Right Shift (CRS) operation to the output of step 3. The number of CRS operations is equal to the random number generation between 1 to 7. The resultant series is represented as 'G'.

Assume random number is 3. Hence we perform CRS operations on 'F' by three times. The resultant 'scrambled parity data' is represented as

$$\therefore \quad G = 11100100000110 \tag{7}$$

- **Procedure for 'Gray Code Data' Generation**

Step 1: First we convert secret data into ASCII values. Then obtained ASCII values are represented in 7-bit binary format. Since, the 'gray-code' and novel 'data conversion' techniques are applicable for only binary sequence.

In this example, the secret information is 'HELLO WORLD'. The ASCII values and 7 bit binary of this example is followed as

H	E	L	L	O	<space>	W	O	R	L	D
72	69	76	76	79	32	87	79	82	76	68
1001000	1000101	1001100	1001100	1001111	0100000	1010111	1001111	1010010	1001100	1000100

Step 2: Now the 'gray-code' technique is applied to each code-word of step 1. The output of the 'gray code' data is given by

1101100 1100111 1101010 1101010 1101000 0110000 1111100 1101000 1111011 1101010 1100110

The gray code technique is used at error correction at receiver side.

- **Procedure for 'Ciphertext' Generation**

Step 1: In order to generate the 'Ciphertext', the first step is to concatenate the output of stage 1 and stage 2. The concatenated data is represented as

11100100000110110110011001111101010110101011010000110000111110011010001111011110101011001 10

Step 2: The resultant data of step 1 is split into 4 bit code-words. If any insufficient bits are remaining in last code-word then complete the code-word by adding with zeros. Since novel 'data conversion' technique is applicable for 4 bit code-words only. The output of step 2 is given

1110 0100 0001 1011 0110 0110 0111 1101 0101 1010 1011 0100 0011 0000 1111 1001 1010 0011 1101 1110 1010 1100 1100

Let the output of step 2 is considered as V. It contains several code-words such as V_1, V_2, V_3,.....V_n. Each code-word contains 4-bits. In above example, V_1=1110. Let consider $V_1(1)$=1, $V_1(2)$=1, $V_1(3)$=1 and $V_1(4)$=0.

Step 3: The novel 'data conversion' technique is introduced in this step to generate the scrambled data. Let

'Vf' denotes the code-word in V, L denotes the output of 'data conversion' technique and 'Lf' denotes the code-word in L. The formula for 'data conversion' technique is given as

$$Lf(1) = Vf(1) \quad (8)$$

$$Lf(2) = \sim(Vf(1)) \& Vf(2) \oplus Vf(1) \& Vf(3) \quad (9)$$

$$Lf(3) = \sim(Vf(1)) \& Vf(2) \oplus Vf(1) \& Vf(3) \oplus Vf(4) \quad (10)$$

$$Lf(4) = Vf(1) \& Vf(2) \oplus \sim(Vf(1)) \& Vf(3) \oplus Vf(4) \quad (11)$$

In above example, V1=1110, then L1 is calculated by using above formula. The result of L1=1111.

Therefore, the output of novel 'data conversion' technique (L) is

1111 0110 0011 1101 0111 0111 0100 1010 0101 1110 1101 0110 0010
0000 1100 1011 1110 0010 1010 1111 1110 1001 1001

Step 4: The output of 'data conversion' technique is converted into 8 bit code-word format. It is represented as

11110110 00111101 01110111 01001010 01011110 11010110
00100000 11001011 11100010 10101111 11101001 1001

Finally, the 8 bit code-words are converted into ACSII value to produce the integer form of encrypted data. The resultant data generated is.

246 61 119 74 94 214 32 203 226 175 233 9

The integer values of this step indicate the ciphertext of the LS encryption algorithm. In this LS (logical & statistical) encryption algorithm, the ciphertext length depends upon the secret text data. The length of ciphertext is expressed as

$$length(ciphertext) <= length(secret\ data) + 1. \quad (12)$$

Taking 60-character secret data as an example then the LS encryption scheme provides 55 length ciphertext. Here, this scheme reduces the ciphertext length rather than the length of secret data. From this result, this scheme helps to improve the payload capacity and quality metrics of the stego image.

3.1.2 Steganography using LWT & RPE Techniques

As shown in above Fig 2. the steganography scheme takes ciphertext and cover image as inputs and generates the stego image. First, the cover image is selected from pool of the images which is available in database. The two-level LWT technique is applied to cover image. On decomposition, it generates LL1, LH1, HL1, LL2, LH2, HL2 and HH2 sub-bands. Next, the ciphertext values obtained from LS encryption algorithm is concealed into HH2 sub-band of cover image by using RPE technique. Finally, stego image is generated with using two level ILWT.

3.2 Receiver Section

The block diagram of receiver section is shown in Fig 3. In receiver section, the steganalysis operation is the first layer. It accepts stego image as an input. In this, the chipertext information is recovered from the stego image. The next layer of receiver section is novel LS decryption algorithm. It takes chipertext as input and finally produces secret data.

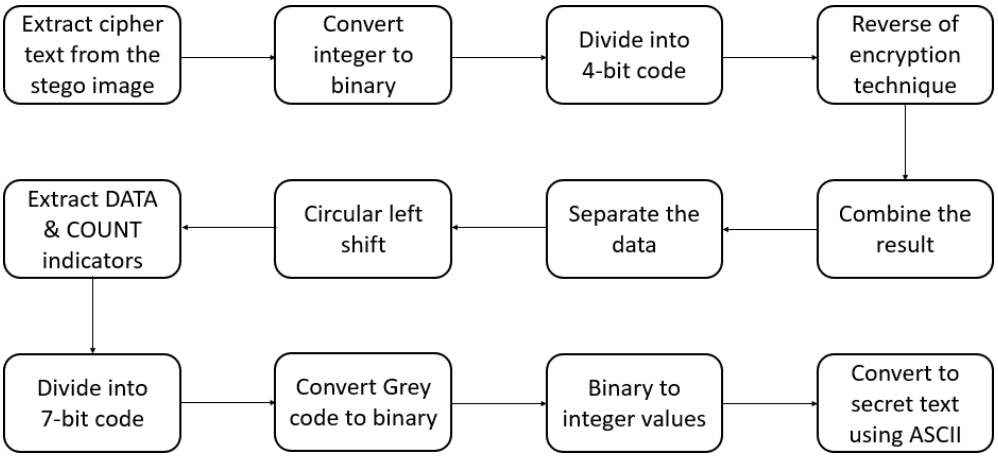


Fig 3. Block diagram of Receiver Section

3.2.1 Steganalysis

The stego image generated from transmitter section is taken as input. Next, the two level LWT technique is applied on stego image in order to retrieve the concealed ciphertext. The resultant ciphertext produced is

246 61 119 74 94 214 32 203 226 175 233 9

3.2.2 LS Decryption Algorithm

As shown in Fig 3. The LS decryption algorithm accepts ciphertext as an input and produces the secret data.

Step 1: The ciphertext obtained from the stego image is converted into 8 bit binary form and it is represented as.

11110110 00111101 01110111 01001010 01011110 11010110
00100000 11001011 11100010 10101111 11101001 1001

Step 2: The output of step 1 is divided into 4 bit code-words. It is represented as

1111 0110 0011 1101 0111 0111 0100 1010 0101 1110 1101 0110 0010
0000 1100 1011 1110 0010 1010 1111 1110 1001 1001

Let the output of step 2 is considered as P. It contains several code-words such as P_1, P_2, P_3,.....P_n. Each code-word contains 4-bits. In above example, P_1=1111. Let consider $P_1(1)$=1, $P_1(2)$=1, $P_1(3)$=1 and $P_1(4)$=1.

Step 3: The reverse process of 'data conversion' technique is introduced in this step. Let 'Pf' denotes the code-word in P, Q denotes the output of this step and 'Qf' denotes the code-word in Q.

The logic for reverse process of 'data conversion' technique is given as

(1)

```
Qf(1)=Pf(1)
```

(2)

```
if (Qf(1)==0)
   if (Pf(2)==0)
     Qf(2)=0
   else
     Qf(2)=1
   end
else
```

(3)

```
if(Pf(3)=Pf(2) ⊕0)
     Qf(4)==0
else
     Qf(4)=1
end
```

(4)

```
if (Qf(1)==0)
   if (Pf(4)==0⊕Qf(4))
     Qf(3)=0
   else
     Qf(3)=1
     end
else
```

```
if (Pf(2)==0)                    if (Pf(4)==0⊕Qf(4))
  Qf(3)=0                          Qf(2)=0
else                             else
  Qf(3)=1                          Qf(2)=1
end                              end
end                              end
```

In above example, P1=1111, then Q1 is calculated by using above logic. The result of Q1=1110. Therefore, the resultant data obtained is

1110 0100 0001 1011 0110 0110 0111 1101 0101 1010 1011 0100 0011 0000 1111 1001 1010 0011 1101 1110 1010 1100 1100

Step 4: The final code-words are obtained from step 3 are concatenated. The resultant data is denoted as 'T'.

T = 1110010000011011011001100111111010101101010110100001100001111100110100011110111101010111001100

Next, the first 14 bits of 'T' are separated and is denoted as 'R'. Since, First 14 bits indicates the 'scrambled parity data' (used in 4.1.1 section). It is used to identify whether received data is correct or not.

R = 11100100000110 (13)

Step 5: Perform 'Circular Left Shift' operation with 3 times to the 'R'. The resultant data is indicated as 'S'. Since 'Circular Right Shift' operation is used in 4.1.1 section.

S = 00100000110111 (14)

Step 6: Reverse bit-stuffing operation is performed on 'S' in order to extract 'data type' and 'count indicator'. Since bit stuffing operation is performed in 4.1.1 section.

Data type = 1011 (Alpha-numeric) Count Indicator = 0000001011 (11-decimal form)

Here, the 'count indicator' indicates the count of the secret data. Hence, based on the 'count indicator' value, we estimated the length of secret data i.e 77 bits (11*7 bits). Since, each character of secret data is represented in 7 bit binary form at transmitter section.

Step 7: The remaining bits of 'T' i.e 15 – 91 bits (77 bits) are separated. These 77 bits are split into 7 bit code-words. The resultant data obtained is.

1101100 1100111 1101010 1101010 1101000 0110000 1111100 1101000 1111011 1101010 1100110

Step 8: Now, 'gray code' to 'binary' conversion technique is applied to step 7 output. The resultant data of step 8 is.

1001000 1000101 1001100 1001100 1001111 0100000 1010111 1001111 1010010 1001100 1000100

Step 9: In step 9, The ASCII values are generated by converting the step 8 output into integer form.

72 69 76 76 79 32 87 79 82 76 68

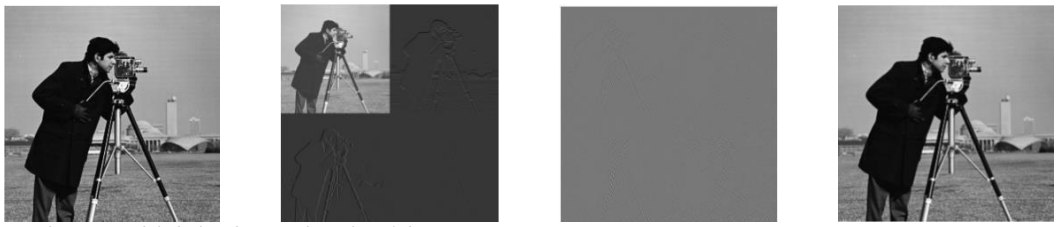
Finally, the secret data produced by converting ASCII value into characters.

H E L L O <space> W O R L D

IV. DISCUSSIONS AND OBJECTIVE ANALYSIS OF RESULTS

The proposed algorithm is written in 'C' language and implemented in MATLAB R 2019b software on VFSRT university computer. Here well known benchmark images are used as a cover images to generate the stego images. These benchmark images are collected from the 'public-domain' [26] and the 'USC-SIPI' images database [27]. Next, the secret data is selected randomly.

First, the proposed method applies LS encryption algorithm on selected secret data to produce the ciphertext. Next, the two-level LWT technique is applied on selected cover image. As a result, LL1, LH1, HL1, LL2, LH2, HL2 and HH2 sub-bands are generated. Let us assume, the cover image is a 'cameraman' whose size is 512 × 512 which is shown in Fig. 4a. Thereafter, the sub-bands of one and two-level LWT is shown in Fig. 4b & 4c. In order to achieve the stego image, the ciphertext is concealed into HH2 sub- band of the cover image which is shown in Fig. 4d.



a) Cover image b) One-level LWT c) Two-level LWT d) Stego image Fig 4. The steganography results of 'Cameraman image'

From the results, the visible difference between stego image (Fig. 4d) and cover image (Fig. 4a) is almost zero. Hence, this algorithm has ability to counteract the supervisory visual attack. Furthermore, this algorithm is also tested with other benchmark images like Barbara, Lena, Coins, Baboon and Pout which is shown in Fig 5. In fact, these images are treated as a cover images. Similarly, the resultant stego images are shown in Fig 6. From these resultant images, secret data is successfully retrieved at receiver using inverse operation of this algorithm which is discussed in section 4.2.

(a) Lena (b)Pout (c) Barbara (d) Baboon (e) Coins

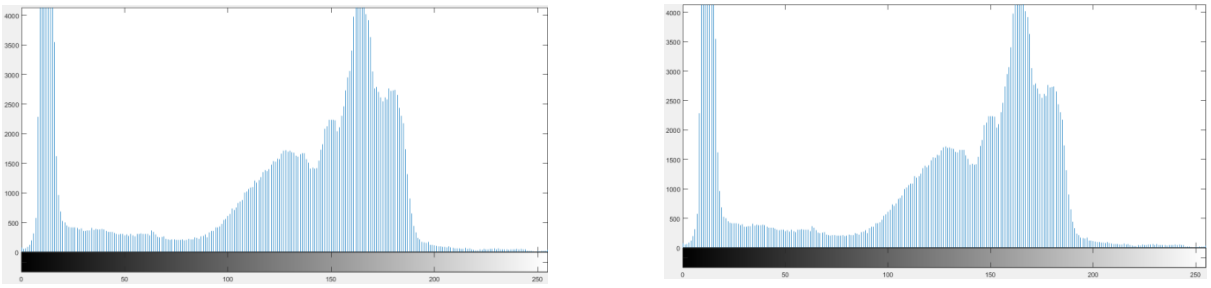
Fig. 5. The cover images.

(a) Lena (b)Pout (c) Barbara (d) Baboon (e) Coins

Fig. 6. The stego images.

V. STATISTICAL ANALYSIS:

The histogram analysis of the cameraman cover and stego image is shown in Fig. 12a and 12b. There is no differences were observed in the histogram images hence they could not be attacked.



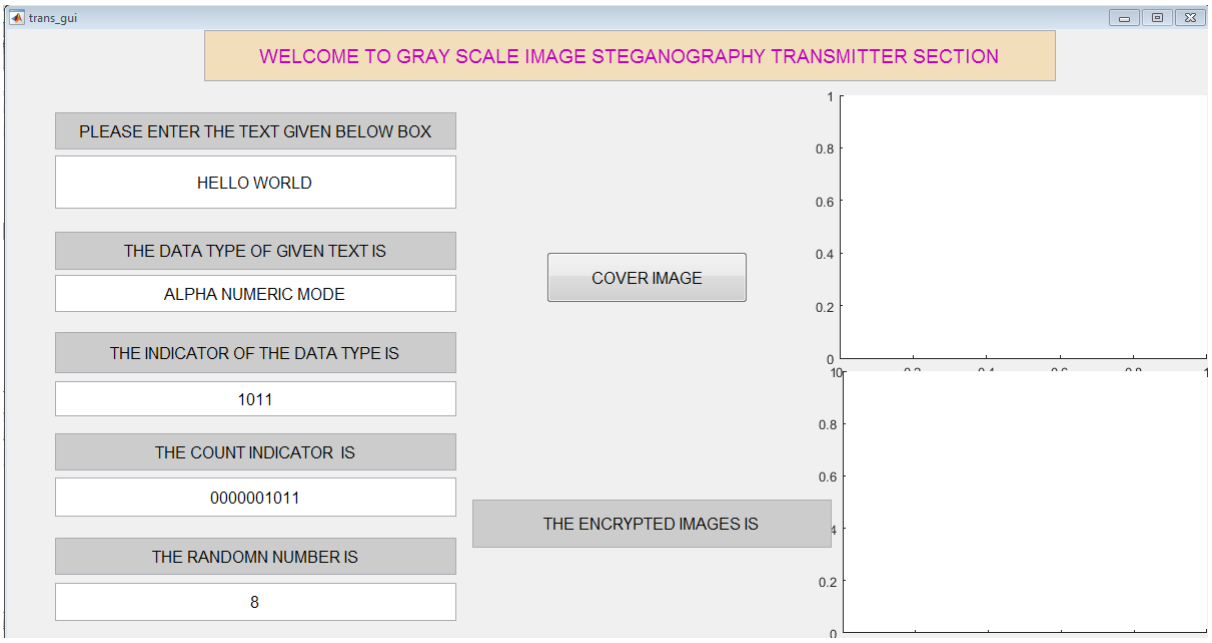
a) Cover image b) Stego image

Fig 12. The histogram analysis of 'cameraman' image

VI. RESULTS

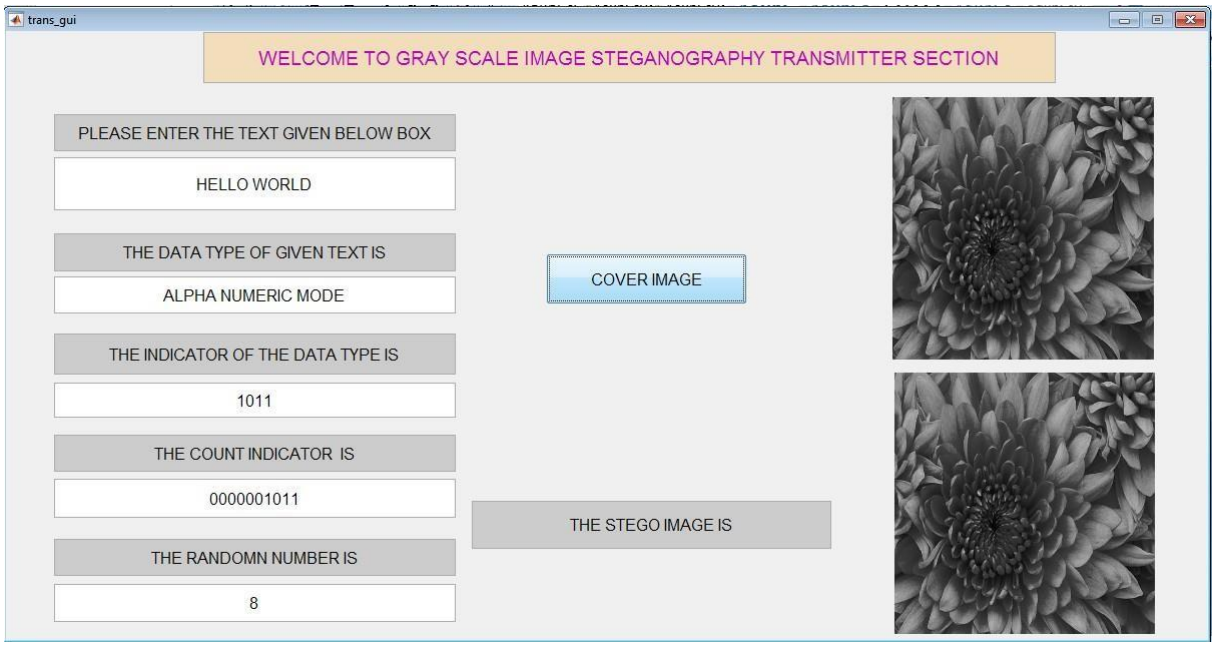
6.1 Transmitter

A The Cover Image of a Steganoraphy is applied as an input to the Image Steganography operation. The secret data can be entered into the corresponding 'Static Box' of theSteganography Transmitter Section

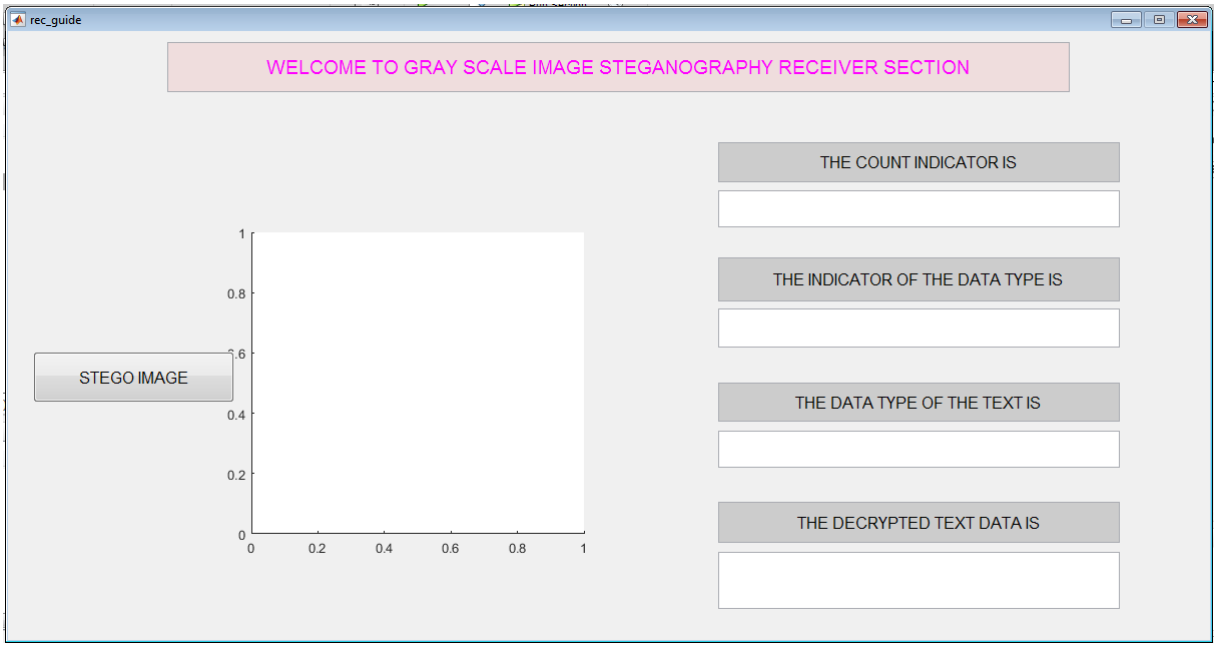


The first level LWT is applied to a cover image then four components are obtained. They are approximation1 (LL1), horizontal1 (LH1), vertical1 (HL1) and diagonal1 (HH1) The second level LWT is applied to a first level LWT image then four components are obtained. They are approximation2 (LL2), horizontal2 (LH2), vertical2 (HL2) and diagonal2 (HH2) components. The stego key is entered into the corresponding 'Static Box' of the Steganography Transmitter Section which is used as a key to obtain the secret data is shown in figure below. The secret characters are converted into decimal values. The decimal

values of the characters are placed in diagonal2 component (HH2) of an image. The starting location of an image is placed in predefined location. The stego image is obtained by applying two levels inverse LWT to LL1, LH1, HL1, HH1, LH2, HL2 and encoded HH2 components. The resultant stego image



6.2 Receiver

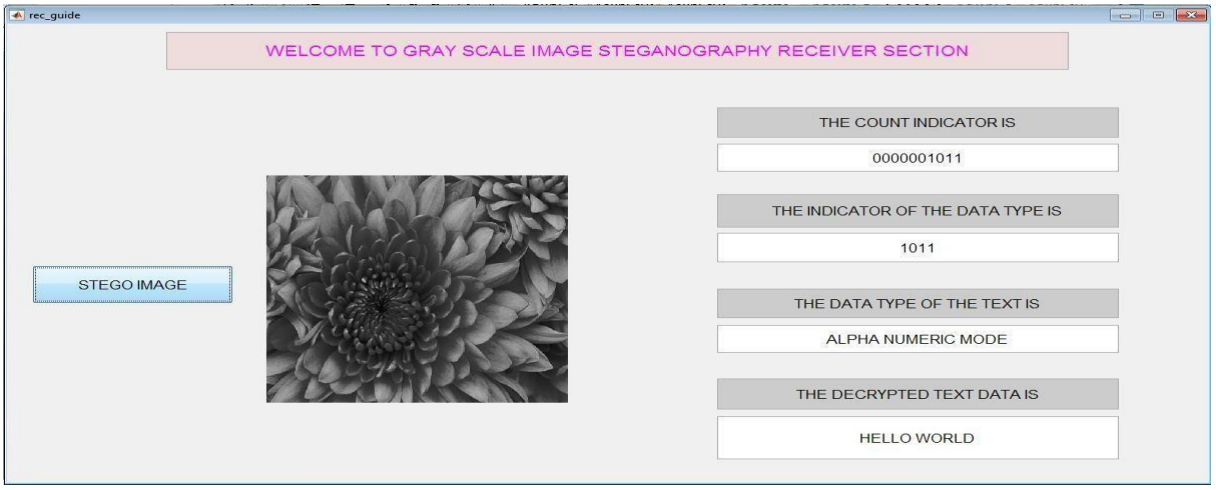


The stego image is selected by click the 'STEGO IMAGE' pushbutton at Steganography Receiver section is shown in figure below

In order to decode the secret data from the stego image, first enter the stego key in correspondent static box and then apply the one level LWT then obtain four components. They are approximation2 (LL2), horizontal2 (LH2), vertical2 (HL2) and diagonal2 (HH2) components

Second levels LWT is applied to the one level LWT image then obtain another four components. They

are approximation2 (LL2), horizontal2 (LH2), vertical2 (HL2) and diagonal2 (HH2) components



The Secret data can be extracted from the diagonal2 (HH2) component. The secret data is obtained in the form of decimal values. These decimal values are converted into characters is shown in figure 8.8. This characters are act as a secret data.

REFERNCES

1. Shuaijianni Xu & Liang Feng Zhang, "Cryptanalysis of Morillo–Obrador polynomial delegation schemes", *IET Information Security,* Volume 12, Issue 2, March 2018, Pp. 127 – 132 https://doi.org/10.1049/iet-ifs.2017.0259
2. Wenying Zhang & Vincent Rijmen, "Division cryptanalysis of block ciphers with a binary diffusion layer ", *IET Information Security,* Volume 13, Issue 2, March 2019, Pp. 87 – 95 https://doi.org/10.1049/iet-ifs.2018.5151
3. Kumar, C., Singh, A.K. & Kumar, P. "A recent survey on image watermarking techniques and its application in e-governance", Multimedia Tools and Applications, 2018, Vol. 77, Pp: 3597–3622. https://doi.org/10.1007/s11042-017-5222-8
4. Y.Eliza Sruthi, A.Rajaiah, M.Govindu, " FPGA Implementation of Lifting DWT Based LSB Steganography", International Journal of Engineering Science and Computing, 2014, Pp: 878-884 DOI:10.4010/2014.260
5. R. De Prisco and A. De Santis, "On the Relation of Random Grid and Deterministic Visual Cryptography", in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 653-665, April 2014. DOI: 10.1109/TIFS.2014.2305574
6. E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform", in *Journal of Systems Engineering and Electronics*, vol. 29, no. 3, pp. 639-649, June 2018. DOI: 10.21629/JSEE.2018.03.21
7. Saeed Sarreshtedari & Mohammad Ali Akhaee, "One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme", *IET Image Processing* , Volume 8, Issue 2, 2014 , p. 78 – 89 https://doi.org/10.1049/iet-ipr.2013.0109
8. Soodeh Ahani & Shahrokh Ghaemmaghami1, "Colour image steganography method based on sparse representation", *IET Image Processing*, 2015, Vol. 9, Iss. 6, pp. 496–50