Received: October 15, 2020. Revised: December 28, 2020. 262

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Improved Dual Steganography Model Using Multi-pass Encryption and Quotient Value Differencing

Shreela Dash[1]* Madhabananda Das[1] Dayal Kumar Behera[2]

[1]*Kalinga Institute of Industrial Technology, Deemed to be University, Patia, Bhubaneswar, India*
[2]*Silicon Institute of Technology, Bhubaneswar, India*
* Corresponding author's Email: shreelamamadash@gmail.com

Abstract: The proposed work suggests a high capacity steganography technique using dual steganography approach. It utilizes a Multi pass encryption system to scramble the mystery message before hiding. The scrambled mystery message is divided into two parts and concealed utilizing two duplicates of the same cover image. One copy of the image uses a modified Quotient value differencing approach to hide 1st part of secret message and another copy uses difference expansion method to embed the 2nd part of secret messages. It provides more secrecy because the suggested work uses the benefits of both encryption and steganography. The investigation shows that the two stego-pictures provide high embedding capability (EC) of 1848153 bits with Peak signal to noise ratio PSNR1 of 47.2 dB and PSNR2 of 51.1 dB. Further, examination with other existing methodologies shows that the suggested methodology is proven to be better in Structural similarity Index (SSIM), EC and PSNR.

Keywords: Steganography, Quotient value differencing, Difference expansion, PSNR, Multi pass encryption.

1. Introduction

Data communication is easier nowadays due to the huge use of the internet. This has drawn the attraction of an immense number of researchers for sharing of information. In any case, correspondence over an open channel is constantly concerned. Keeping the secrecy of data from the unauthorized users is the prime goal, cryptography and steganography assumes a predominant job to accomplish security. Steganography is an approach of communicating secret messages through the insecure channel. It is performed by embedding the mystery information inside picture, sound, and video documents [1]. In this technique the characteristics of the picture like histogram, SSIM must remain unchanged ensuing to covering the secret data in it [2]. Cryptography is a method which protects the secret information by encrypting them, so that only the authorized user can read it [4]. Steganography provides secret communication, so that no one can identify the presence of covert message and cryptography is the method used for encryption of secret message so that unauthorized user can not break it. In this paper both the cryptography and steganography approach is combined to add more secrecy to the secret communication. There exists a huge number of existing techniques in the literature but there is still scope of significant upgrades to have high Embedding limit and secrecy to mystery message.

In the proposed work, utilizing hybridization of both cryptography and steganography a high secrecy correspondence is done. The proposed strategy improves the Embedding limit by hiding the secret data in dual image utilizing QVD and Difference expansion method. Our proposed work is based on spatial domain principle as it gives emphasis to the high payload of secret data. We observed that the payload capability and the security are still less in the existing methods. So the suggested approach uses the concept of Dual steganography to increase the capability of embedding and cryptography approach for improving secrecy of hiding.

The significant enhancements of the proposed methods are given below:

1. The proposed approach encrypts the secret message using Multi-pass encryption (MPE) technique before embedding.
2. The proposed approach effectively utilizes the two similar images efficiently for the concealing of secret information. Both the stego images are then needed to fully extract the hidden data.
3. Using QVD and DE technologies, the technique effectively hides more mysterious bits to strengthen the embedding capability.

The organization of the work is sorted out as given below. Section 2 surveys existing methodologies present in a similar area. The proposed strategy is presented in Section 3. In Section 4 the outcomes and relative analysis is introduced. At last, Section 5 describes the final outcomes.

2. Literature survey

Major research on image steganography has been performed over the years. These algorithms are categorized into two main classes depending on embedding method i.e. spatial domain [6, 7, and 11] and transform domain. The spatial domain embedding algorithms are used frequently because of their good concealing technique, more capacity to hide information, and simplicity of understanding [5]. LSB and pixel value difference are the most common methods in the spatial domain [2]. Some of the works in the same domain are studied in literature. The LSB matching of Mielikainen [10] is one of the typical works in this area that results in stego image with the least possible distortion of stego image. The process was nevertheless reversible. By expanding the LSB matching strategy, Lu *et al.* [5] uses a table of rules to preserve the quality of image. By using twin images, the HC of the technique has been doubled. However, Lu's technique can be further improved in terms of capacity. A novel steganographic framework depends on the techniques of PVD and modified LSB is suggested in [8]. The main contributions are to increase the amount of embedded data and with accepted distortion. However, in high EC the PSNR is nearly 35, which can be improved. Jung *et al.* [9] have used two similar images for embedding to improve capacity. Mean and adjacent pixel difference are used to maintain reversibility. The Embedding capacity using dual cover image can be further improved. In [12] the authors have combined both differencing and substitution mechanisms for better performance in high capacity steganography. Firstly, the image is partitioned into independent pixel blocks of size 3×3 and on every pixel block, LSB substitution is applied on the two least significant bits and QVD is applied on the rest of the bits. The technique results in degrade of quality of stego image. H. Yuan [13] have used multiple cover images using Secret Sharing method and the suggested approach hide the encrypted bits adaptively in each cover. The suggested method results in FOBP (Fall of Boundary Problem). A method proposed by Tseng [14] hides the secret message using the edge by deciding the number of pixels to be hidden using LSB technique. It enhances the capability of hiding but the security of the technique can be further improved. Nguyen [15] has suggested adaptive LSB based MPBDH technique that uses both smooth and rough region for data hiding. To detect the complex regions of a cover image for embedding the confidential message, it uses more no. bit plane and used an adaptive complexity threshold. The embedding power and protection quality have improved dramatically relative to the previous system. Another method suggested by [16] combining directional PVD with LSB that results improvement in PSNR with high payload. F. Jafar *et al.* [18] suggested a RDH approach where embedding and extraction of data is performed in three consecutive steps. In the initial step, one mystery bit in every pixel is inserted utilizing four straightforward principles. The other two stages utilize the idea of prediction for inserting mystery information yet without utilizing any unpredictable indicators. However, the hiding limit can be additionally improved.

3. Proposed work

New steganography approaches are in current progressions and research is still going on for enhancing capacity of payload with more security and less distortion. The suggested work aims at enhancing the embedding capability and to maintain the secrecy of the communication. In the proposed approach, authors combined both the cryptography and steganography approach and get the benefits of both the techniques. To improve the secrecy of covert communication encryption technique is used and steganography methods help for secret communication. For improving the capacity of embedding algorithm, dual stego images are used. It not only improves capacity but also improves secrecy as to retrieve the secret information both the stego images are required. The proposed approach is represented in Fig. 1.

Proposed dual steganography method

1. The secret message S is encrypted using Multi pass Encryption (*MPE*) algorithm.

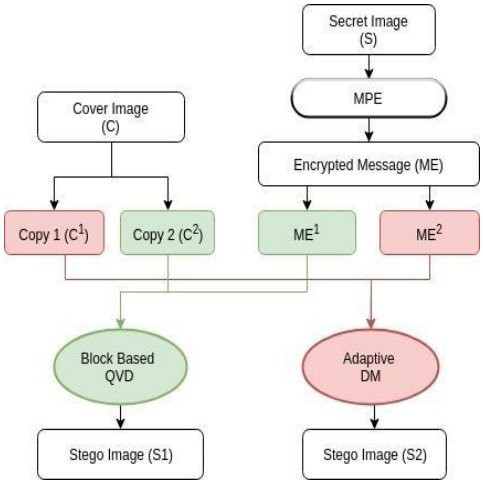

Figure. 1 The proposed dual steganography approach

2. The encrypted message *ME* is divided into 2 parts. Odd indexed elements are kept in ME^1 and even indexed elements are kept in ME^2.
3. Two identical copies of the cover image *C* are taken i.e. Copy1 (C^1) and Copy2 (C^2) respectively.
4. ME^1 is implanted in the cover image C^2 by block QVD technique and ME^2 is embedded in C^1 using Adaptive Difference Modification technique.
5. Two generated stego images *S1* and *S2* are transferred through the communication medium.

3.1 Multi pass encryption algorithm

The Secret message is encrypted using the following algorithm. The algorithm contains 4 steps.

Input: Secret message(S)

Output: Encrypted message (ME)

1. In the first step each 8 bits of secret message S is taken and XOR operation with *11111111* is performed.
2. The 8 bit of the secret message is divided into 4 blocks. Each block consists of 2 bits. The division is done in the following way. *s1* = 5^{th} and 1^{st} bit of each 8 bit, *s2*= 6^{th} *and* 2^{nd} bit, *s3*= 7^{th} *and* 3^{rd} bit. *s4*= 8^{th} *and* 4^{th} bit. The 4 blocks are concatenated.
3. Then the shuffling of the secret bits is done using some random secret key k. The k is of length 8 and it consists of 1 to 8 decimals.
4. The random secret binary key k is taken for encryption. If k_i *=1*, then XOR operation with the particular bit of secret message is done otherwise it is left unchanged.

The idea of MPE algorithm is explained with a simple example.

Consider the 8-bits of secret message S= *10011011*.

Figure. 2 Illustration of generation of encrypted secret message

As per step 1 *XOR* operation of the Secret message S with *11111111* is performed.

S=10011011 XOR 11111111=01100100

As per step 2 the secret message S is divided into 4 blocks i.e. S_1*=11,* S_2*=00,* S_3*=10,* S_4*=11*. After concatenation of the four blocks *SS = 11001011*.As per step 3 the random secret key is generated for example:"*41273865*". As 1^{st} position of secret key is 4 so 1^{st} *bit* of *SS* i.e. 1 is placed in 4^{th} position and so on. After step 3 the generated secret message is *SS= 10111100*. As per step 4 random binary secret key is taken i.e. *k=01100110*. If k_i *=1* XOR operation of *SS* is performed with the corresponding bit of *k* otherwise no operation is performed. The generated encrypted secret message is *ME=11011010*.

The illustration after each step is shown in Fig.2.

For decryption of the encrypted message, the receiver will perform the above 4 steps in reverse order.

3.2 Embedding technique

The cover image *C* is copied and two same share of the cover image C^1 and C^2 are made. The scrambled secret message is partitioned into two parts. The odd indexes of *EC (ME in Fig. 1)* are kept in one array EC^1 and even index numbers are kept in EC^2. The EC^1 is embedded in cover image C^1 using block based QVD technique and EC^2 is embedded using adaptive DE technique. Then the dual stego images are transferred through the unsecure communication channel.

3.2.1. Embedding using block based QVD

Input: Identical copy of the cover image C^1 *(I1, I2, I3, ……, In)* and the covert message EC^1.

Output: The stego image S^1

Algorithm

1. The original image C^1 is partitioned into *3×3* size blocks. From the block using Eq. (1) and Eq. (2) the high order and low order bits of each pixel of the block are separated.

$$q_i = I_i \; div \; 4 \quad for \; i = 1 \; to \; 9 \qquad (1)$$

$$r_i = I_i \; mod \; 4 \quad for \; i = 1 \; to \; 9 \qquad (2)$$

Table 1. Range table

Range ($L_i - H_i$)	0-7	8-15	16-31	32-63
Capacity(m_i)	2	3	4	5

Where q_c and r_c are the centre pixel of each block.

2. Retrieve each 2 bits of secret message from EC^1 and convert it to decimal b_i. Each pixel of r_i will be replaced with b_i.

$$r_i' = b_i \quad for\ i = 1\ to\ 9 \tag{3}$$

3. For each high order pixel in q_i, find the difference d_i with centre pixel q_c using Eq. (4).

$$d_i = q_i - q_c \quad for\ i = 1\ to\ 9 \tag{4}$$

4. According to the range of distance values given in Table 1, the capacity of each pixel to hide (m_i) is found. m_i Bits of secret data from EC^1 are transformed to decimal b_i .The modified difference d_i' is calculated using Eq. (5).

$$d_i' = \begin{cases} L_i + b_i & \text{if } d_i \geq 0 \\ -L_i - b_i & \text{if } d_i < 0 \end{cases} \tag{5}$$

5. Then the difference between modified difference and original difference is calculated using Eq. (6).

$$k_i = d_i' - d_i \tag{6}$$

6. Then q_i' is calculated using using Eq. (7)

$$q_i' = q_i + k_i \tag{7}$$

7. The stego pixels are calculated using Eq. (8)

$$S^1(i) = q_i' \times 4 + r_i' \quad for\ i = 1\ to\ 9 \tag{8}$$

3.2.2. Embedding using adaptive DE

Input: Identical copy of the cover image C^2 (J1, J2, J3,…….., Jn) and the covert message EC^2.

Output: Stego imageS^2.

Algorithm

1. Divide C^2 into independent blocks of size 3×3.
2. Each 3 bits of secret message from EC^2 is converted to decimal b_i. Each pixel is converted to binary and the last 3 bits are converted to decimal p_i.
3. Find the difference d_i using Eq. (12).

$$d_i = p_i - b_i \tag{12}$$

4. Modified pixels j_i', j_i'', j_i''' are found using Eqs. (13), (14), and (15) respectively.

$$j_i' = j_i - d_i \tag{13}$$

$$j_i'' = j_i - 2^3 \tag{14}$$

$$j_i''' = j_i + 2^3 \tag{15}$$

5. The stego-pixel $S^2(i)$ is calculated using Eq. (16).

$$S^2(i) = min\ (j_i', j_i'', j_i''') \tag{16}$$

3.3 Extraction technique

The dual stego images S^1 and S^2 are transferred through the communication medium. From both the stego images the covert bits are generated to get the scrambled message. The reverse steps of multi pass encryption are performed to generate original secret message. .

3.3.1. Extraction algorithm for QVD

Input: Stego-image received through communication channel S^1.

Output: The encrypted message EC^1.

Algorithm

1. The stego-image $S^1$is split into 3×3 independent blocks. Then the high-order and low-order bits are generated using Eq. (9) and (10), respectively.

$$q_i = S^1(i)\ \text{div}\ 4 \quad \text{for i} = 1 \text{ to } 9 \tag{9}$$

$$r_i = S^1(i)\ \text{mod}\ 4 \quad \text{for i} = 1 \text{ to } 9 \tag{10}$$

2. Each pixel in r_i is transformed to binary and retrieve the last 2 bits of each pixel add it to EC^1.
3. For each block q_i , the difference of each quotient pixel with the centre pixel is calculated using Eq. (11).

$$d_i = q_i - q_c \tag{11}$$

4. For each d_i we can generate L_i and capacity m_i using the Table 1. b_i' is calculated and is transformed to m_i binary bits and are appended to EC^1.

3.3.2 Extraction algorithm for adaptive DE

Input: Stego-image received through communication channel S^2.

Output: The encrypted message EC^2.

Algorithm

1. The stego-image S^2 is split into 3×3 independent blocks.
2. Convert pixels of each block to binary and retrieve 3 LSB bits.
3. Append these bits to the extracted bits EC^2.
4. Then EC^1 and EC^2 are arranged in an odd and even position sequentially to generate the encrypted message *EC*.

3.4 Illustration of embedding and extraction algorithm

To explain the embedding and extraction algorithm, we use a 3×3 block given in Fig. 3. The encrypted secret bit *EC* is divided into 2 parts

EC^1 =100110110101001101110011011

EC^2= 101110010100011100100101000

170	160	149
171	158	173
173	173	170

42	40	37
42	39	43
43	43	42

2	0	1
3	2	1
1	1	2

Figure. 3 Original block, high order and low order pixel values

42	39	42
41	39	41
40	42	41

2	1	2
3	1	1
0	3	1

170	157	170
171	157	165
160	171	165

Figure. 4 High order, Low order pixel values and generated stego block

170	160	149
171	158	173
173	173	170

162	154	152
170	155	175
173	173	170

Figure. 5 Original block and corresponding stego block

As per the algorithm the high-order and low-order bits are calculated as per Eqs. (1) and (2) which is given in Fig. 3.

Two secret bits from EC^1 are converted to decimal and set as values in r_i' . Then as per Eq. (4) the difference between q_i and q_c is calculated. So, $d_1=3$, $d_2=1$, $d_3=-2$, $d_4=3$, $d_5=4$, $d_6=4$, $d_7=4$ and $d_8=3$. Now from Table 1 we found the difference di is within the range 0 to 7, Lower index L_i =0 and capacity m_i=2. As the hiding capacity is 2, 2 bits of secret data are converted to decimal i.e. $b_1=3$, $b_2=0$, $b_3=3$, $b_4=1$, $b_5=2$, $b_6=1$, $b_7=3$, $b_8=2$. The modified difference d_i' is calculated using L_i and b_i. So $d_1'=3$, $d_2'=0$, $d_3'=3$, $d_4'=1$, $d_5'=2$, $d_6'=1$, $d_7'=3$, $d_8'=2$. Then difference between di and d_i' calculated and kept in ki. So $k_1=0$, $k_2=-1$, $k_3=5$, $k_4=-2$, $k_5=-2$, $k_6=-3$, $k_7=-1$ and $k_8=-1$. The modified q_i' is calculated as per Eq. (7). The values are $q_1'=42$, $q_2'=39$, $q_3'=42$, $q_4'=41$, $q_5'=41$, $q_6'=40$, $q_7'=42$, $q_8'=41$. As per Eq. (8) the calculated stego pixels along with high order and low order bits are shown in Fig. 4.

After getting the first stego block, the second pair of secret bits EC^2 is hidden inside the original block using Adaptive DE algorithm. Here 3 bits of secret message are converted to decimal and kept in b_i. So, $b_1=5$, $b_2=6$, $b_3=2$, $b_4=4$, $b_5=3$, $b_6=4$, $b_7=4$, $b_8=5$, $b_9=0$. Then the last 3 bits of each pixel in the block are converted to decimal and kept in p_i. So $p_1=2$, $p_2=0$, $p_3=5$, $p_4=3$, $p_5=6$, $p_6=5$, $p_7=5$, $p_8=5$, $p_9=2$. The d_i is calculated as per Eq. (9). So $d_1=-3$, $d_2= -6$, $d_3=3$, $d_4= -1$, $d_5=3$, $d_6=2$, $d_7=1$, $d_8=0$ and $d_9=2$. The generated stego block is calculated and given in Fig. 5.

The receiver will take out the mystery bits from the generated stego images S^1 and S^2. From S^1 the high order bits (q_i') and low order bits (r_i') are generated. Each pixel r_i' of the block is converted to 2 bits binary and added to the 1D array EC^1. Then from (q_i') the difference d_i' is calculated. The calculated values are $d_1'=3$, $d_2'=0$, $d_3'=3$, $d_4'=1$, $d_5'=2$, $d_6'=1$, $d_7'=3$, $d_8'=2$. From Table (1) the range is found. Here $L_i=0$ and $m_i=2$. So the values are $b_1=3$, $b_2=0$, $b_3=3$, $b_4=1$, $b_5=2$, $b_6=1$, $b_7=3$, $b_8=2$ and each b_i is converted to 2 bit binary and appended to EC^1. Similarly from S^2 the last 3 binary bits of each pixel are generated and appended to EC^2. Now EC^1 and EC^2 are combined to generate the encrypted secret message EC.

4. Result analysis

The experiment was conducted utilizing MATLAB R-2017. The original images were chosen

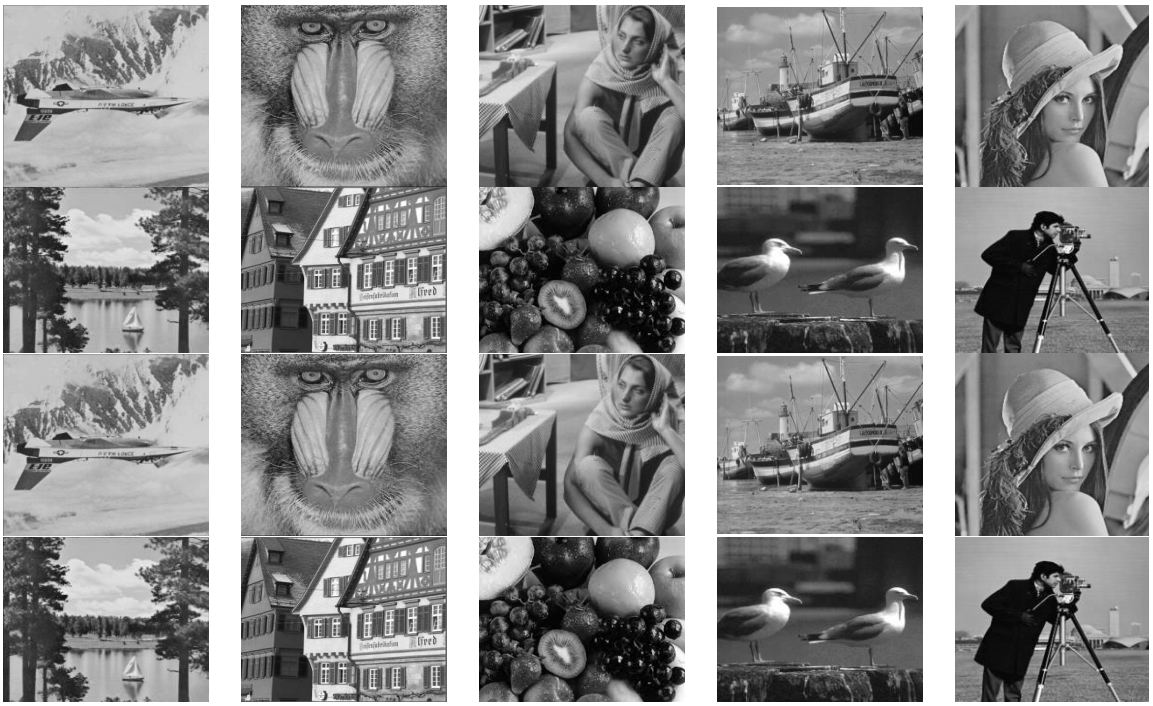

Figure. 6 Cover image and corresponding stego image

Table 2. Analysis of Proposed method and Jung's [9] method

Test Image (512x512)	Proposed Technique				
	EC	PSNR1	PSNR2	SSIM1	SSIM2
Airplane	18,21,220	48.3	52.2	0.9987	0.9989
Boat	18,67,436	46.6	52.0	0.9992	0.9986
House	18,67,436	46.6	49.9	0.9989	0.9997
Scenery	18,50,455	46.9	51.0	0.9986	0.9992
Lena	18,60,400	47.1	49.9	0.9987	0.9988
Baboon	18,21,220	48.3	52.1	0.9978	0.9980
Zelda	18,67,436	46.8	50.2	0.9991	0.9993
Bird	18,60,670	47.3	50.0	0.9987	0.9987
Cameraman	18,35,008	48.1	51.8	0.9982	0.9984
Fruit	18,30,250	48.2	51.9	0.9983	0.9983
Average	18,48,153	47.2	51.1	0.9986	0.9988

Test Image (512x512)	Jung's [9]				
	EC	PSNR1	PSNR2	SSIM1	SSIM2
Airplane	7,81,964	45.5	47.4	0.9857	0.9865
Boat	7,86,097	45.4	47.5	0.9906	0.9886
House	7,79,948	45.5	47.4	0.9922	0.9902
Scenery	7,70,943	46.9	51.0	0.9887	0.9880
Lena	7,73,666	45.4	47.4	0.9860	0.9885
Baboon	7,72,544	45.5	47.5	0.9878	0.9980
Zelda	7,85,008	45.3	47.4	0.9880	0.9850
Bird	7,65,090	45.5	47.1	0.9887	0.9967
Cameraman	7,65,312	45.5	47.2	0.9880	0.9859
Fruit	7,60,506	45.5	47.3	0.9883	0.9873
Average	7,74,107	45.6	47.7	0.9884	0.9895

from USC-SIPI image databases with a size of 512x512 pixels [17]. The original and stego images are given in Fig. 6. The suggested technique is implemented and compared with the existing methodologies in the same domain [3,5,9]. The work used the (PSNR) to measure the pixel gap between stego images and the original image.

Table 3. Result of Lu's [5] and Qin's [3] method

Test Image (512x512)	LU's [5]				
	EC	PSNR1	PSNR2	SSIM1	SSIM2
Airplane	5,24,288	49.11	49.09	0.9983	0.9985
Boat	5,24,208	49.14	49.09	0.9989	0.9986
House	5,24,996	49.15	48.86	0.9981	0.9982
Scenery	5,24,288	49.11	49.1	0.9985	0.9987
Lena	5,24,288	49.13	49.12	0.9987	0.9988
Baboon	5,22,240	49.14	49.09	0.9983	0.9985
Zelda	5,24,996	49.13	49.12	0.9991	0.9993
Bird	5,24,280	49.11	49.14	0.9967	0.9972
Cameraman	5,22,244	49.03	49.11	0.9980	0.9982
Fruit	5,22,240	49.13	49.09	0.9983	0.9984
Average	5,23,806	49.11	49.08	0.9983	0.9984

Test Image (512x512)	Qin's[3]				
	EC	PSNR1	PSNR2	SSIM1	SSIM2
Airplane	5,57,339	41.55	52.12	0.9867	0.9885
Boat	5,57,194	41.57	52.11	0.9866	0.9886
House	5,57,948	41.48	51.91	0.9867	0.9882
Scenery	5,57,564	41.58	52	0.9870	0.9880
Lena	5,57,552	41.58	52.11	0.9867	0.9884
Baboon	5,57,264	41.34	52.12	0.9863	0.9878
Zelda	5,57,948	41.48	52.1	0.9867	0.9881
Bird	5,57,552	41.48	52.11	0.9871	0.9882
Cameraman	5,57,948	41.11	51.91	0.9863	0.9879
Fruit	5,57,260	41.19	52.15	0.9870	0.9878
Average	5,57,556	41.43	52.06	0.9867	0.9882

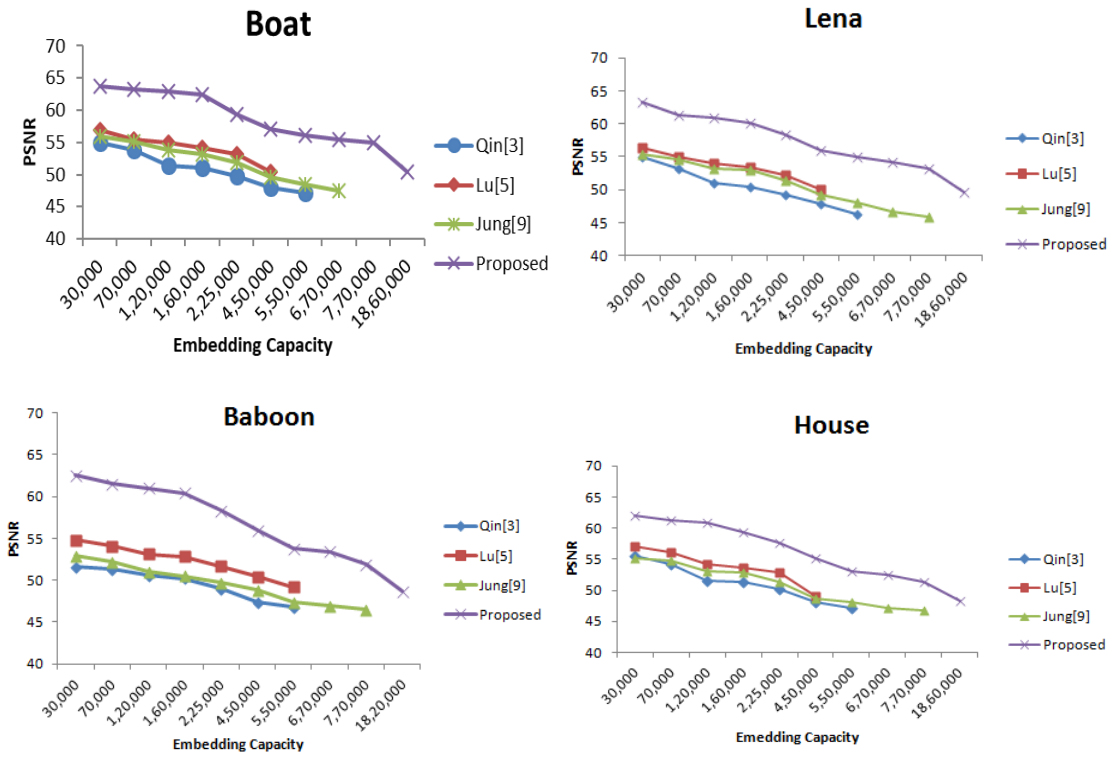

Figure. 7 EC vs PSNR of different test images

$$PSNR = 10log_{10}\frac{Max^2}{\frac{1}{m\times n}\sum_{i=1}^{n}\sum_{j=1}^{n}(C_{ij}-S_{ij})^2} \quad (17)$$

Here *Max* is used to denote the maximum intensity value in the image. c_{ij} and s_{ij} represent the corresponding pixels of the Test and Stego image respectively. The performance of the algorithm is also evaluated based on different parameters like Embedding capacity and Structural similarity Index. SSIM value close to 1 increases stego-image efficiency [2]. The SSIM can be evaluated using Eq. (18).

$$SSIM=\frac{(2\overline{p}q+C_1)(2\sigma_{pq}+C_2)}{\left(\overline{p^2}+\overline{q^2}+C_1\right)(\sigma_p{}^2+\sigma_q{}^2+C_2)} \quad (18)$$

$\overline{\mathrm{p}}, \overline{\mathrm{p}^2}$, $\sigma_{\mathrm{p}}{}^2$ and $\overline{\mathrm{q}}$, $\overline{\mathrm{q}^2}$, $\sigma_{\mathrm{q}}{}^2$ reprsent the mean, variance and the standard deviation of the the original and stego image respectively. Likewise $2\sigma_{\mathrm{pq}}$ is the covariance and the two constants are c_1 and c_2.

The comparison of the stego image in the suggested approach with the existing Jung's [9] technique is shown in Table 2. Here PSNR1, PSNR2, SSIM1 and SSIM2 represent the PSNR and SSIM value of the 1st stego-image, 2nd stego-image respectively. Table 2 shows SSIM value is nearly equal to 1 for all the test images taken. The PSNR, Embedding capacity and SSIM of the existing approach Qin's [3] and Lu's [5] is given in Tables 3. The result analysis shows that the embedding capability of the suggested technique is much more higher than the other existing techniques of same domain. For ex: Boat image has hiding capacity of 18, 67,436 with PSNR1 46.6 and PSNR2 is 50 in proposed method where as in Jung [9] the hiding capacity is 7,86,097 with PSNR1 is 45.5 and PSNR2 is 47.4. In Lu [5] the hiding capacity is 5,24,208 with PSNR value 49 and Qin [3] provides 5,57,194 hiding capacity with PSNR1 41.57 and PSNR2 52.11. The average embedding capability of the proposed method is 18,48,153 which is much more than the other existing methodologies shown in Table 2.

Similarly SSIM1 and SSIM2 of images shown in Table 2 and Table 3 also prove that SSIM value of the suggested approach is higher than the existing methods. Average SSIM1 of proposed method is 0.9986 and PSNR2 is 0.9988 which is nearly equal to 1 which shows that the image quality is better.

Fig. 7 shows the relation of embedding capability with PSNR for 4 different images Lena, Boat, House and Baboon. The result shows that with increasing embedding capacity PSNR decreases. It also shows with embedding capacity 30000 bits the proposedmethod results in PSNR value more than 60 whereas Jung's [9], Lu's [5] and Qin's [3] exhibits PSNR value more than 50.

5. Conclusions

A high capacity information hiding technique is proposed using Multi pass encryption, QVD and adaptive DE technique. The secret message is scrambled using MPE technique to use the benefit of cryptography and providing more secrecy. The dual images of same cover image is obtained and used to conceal the encrypted secret message. QVD technique is used to hide the part of secret message in 1st cover image and adaptive DE technique is used to embed the rest part in 2nd cover image. The proposed method provides the embedding capacity of 18,48,153 with PSNR1 47.2 and PSNR2 52.1 in average for the Test images. The comparison is also done with the existing techniques of same domain and the result shows that the proposed technique has improved EC, PSNR and SSIM. In the future the capacity can be further improved by identifying the features of each block to generate the capacity of hiding. The proposed work will be further extended to validate for unauthorized attack.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, methodology, software, investigation, validation, writing—original draft preparation, writing and editing, S. Dash; investigation, review, supervision, M.N. Das; resources, formal analysis, writing—review and editing, D.K. Behera.

References

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", *Neuro computing*, Vol. 335, pp. 299-326, 2019

[2] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey", *Signal Processing: Image Communication*, Vol. 65, pp. 46-66, 2018.

[3] C. Qin, C. Chang, and T. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images", *Multimed Tools Appl*, Vol. 74, pp. 5861–5872, 2015.

[4] S. Dash, M. N Das, and M. Das, "Secured Image Transmission through Region-Based

Steganography Using Chaotic Encryption, Computational Intelligence in Data Mining", *Advances in Intelligent Systems and Computing*, Vol. 711. Springer, 2018

[5] T. Lu, C. Tseng, and J. Wu, "Dual imaging-based reversible hiding technique using LSB matching", *Signal Processing*, Vol. 108, pp. 77-89, 2015,

[6] A. Zakaria, M. Hussain, A. Wahab, M. Idris, N. Abdullah, and K.-H. Jung, "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution", *Applied Sciences*, Vol. 8, No. 11, 2018.

[7] J. Wang, J. Ni, X. Zhang, and Y. Q. Shi, "Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting", *IEEE Transactions on Cybernetics*, Vol. 47, No. 2, pp. 315-326, 2017.

[8] K. A. Darabkh, A. K. Al-Dhamari, and I. F. Jafar, "A new steganographic algorithm based on multi directional PVD and modified LSB", *Journal of Information Technology and Control*, Vol. 46, No.1, pp. 16-36, 2017.

[9] K. H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing", *The Imaging Science Journal*, Vol. 63, No. 7, pp. 398-407, 2015.

[10] J. Mielikainen, "LSB matching revisited", *IEEE Signal Processing Letters*, Vol. 13, No. 5, pp. 285-287, 2006.

[11] T.-C. Lu, C.-Y. Tseng, S.-W. Huang, and T. Nhan, "Pixel-Value-Ordering based Reversible Information Hiding Scheme with Self-Adaptive Threshold Strategy", *Symmetry*, Vol. 10, No. 12, p. 764, 2018.

[12] G. Swain, "Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution", *Arabian Journal for Science and Engineering*, Vol. 44, No. 4, pp. 2995–3004, 2019.

[13] H. D. Yuan, "Secret sharing with multi-cover adaptive steganography", *Information Sciences an International Journal*., Vol. 254. pp. 197-212, 2014.

[14] H. Tseng and H. Leng, "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion", in *IET Image Processing*, Vol. 8, No. 11, pp. 647-654, 2014.

[15] T. D. Nguyen, S. Arch-int, and N. Arch-int "An adaptive multi bit-plane image steganography using block data-hiding", *Multimedia Tools Appl*, Vol. 75, pp. 8319–8345 ,2016.

[16] G. Swain, "A steganographic method combining LSB substitution and PVD in a block", *Procedia Comput. Sci*., Vol. 85, pp. 39–44, 2016.

[17] USC-SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc. Accessed 19 2019.

[18] F. Jafar, K. A. Darabkh, R. T. Al-Zubi, and R. R. Saifan, "An efficient reversible data hiding algorithm using two steganographic images", *Signal Processing*, Vol. 128, pp. 98-109, 2016.