ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 4, April 2021

An Enhancement of Digital Image Steganography Based on a PVD and Modulo Operation

[1] Manoj Kumar Sharma, [2]Monika Sharma, [3]Prem Kishor Gautam
[1][3] Assistant Professor, Department of Computer Science & Engineering, MIT Bulandshahr UP, India
[2]M.Tech Scholar, Department of Computer Science & Engineering, MIT Bulandshahr UP, India

Abstract: Digital Technology rapidly increases the system technology for sending information securely. The internet as a whole does not use secure link, thus the information in transmit may be vulnerable to interception as well. It is important to reduce the chance of information being detect during transmission. Image steganography is the best solution for providing security during the transmission. In this paper, we enhance some image steganography techniques used to increase image hiding capacity, increase peak-signal-noise-ratio value and also avoidance fall off boundary problems that is based on pixel value difference and modulo operation us. In this proposed work, we separated image into 1*4 pixels and secret data binary bit embed in a pixel blocks using pixel difference modulo operation (PDMO) and find average pixel value difference (APVD) readjustment. In PDMO, we find difference between starting three consecutive pixels of a block using a range table. In this phase modulo operation (MO) use for embedding secret bit into these blocks. Now average of the starting three stego-pixels and the last pixel of the block are considered for data embedding using PVD method. The result of the proposed work has been compared with other approaches and found to be improved. In this proposed work, shows quality and PSNR value between cover image and stego-image. The main aim of this paper is that do not losses image quality during transmission.

Keywords: - Steganography, average pixel value difference (APVD), modulo operation (MO), pixel difference modulo operation (PDMO), capacity.

1. INTRODUCTION

Data security system protects and secures data from unauthorized person. The terms data security, information security, system security are being used interchangeably. Data Secure in physical and administrative area. Most of computers has no and very little bit secures but day by day realized importance of security. In this way, to protect data confidential and give authenticity properly is very important. Data hiding security system play important part for deliver data securely from sender to receiver. Cryptography and Steganography technique mostly used to protect the data from unauthorized party. Steganography technique is the art of hiding data and covert communication between sender and receiver. Steganography conceal the data inside an image, audio, video or text. Image steganography mostly used to hide the secret data in an image. Many image steganography techniques used in spatial domain are LSB substitution, gray level modification, Pixel vale differencing and so on. This proposed scheme uses PVD algorithm for find the average difference value between original image and stego-image.

Pixel value difference (PVD) and modulo function (MF) also used for resolved the boundary problem in pixels and avoid fall off boundary problem. PVD only used a pair of pixels. The name of pair implies; horizontal, vertical and diagonal. This technique applied between images (24*24) as well as image (1024*1024). In this technique, information cannot directly hide into pixel. Pixel is hidden into the first pixel of PVD. Pixel value difference selected any two pixel value of image and it calculates nearest pixel value. Calculation between two image pixel values by using histogram analysis is known as selected channel. And the last result shows PSNR is higher than MSE value. Histograms graphical represent minimum pixel difference between two images.
of embedding capacity and preserving stego-image quality.
Wu and Tsai in 2003 was proposed steganography technique is pixel value differencing (PVD). In this technique, image separated into different non-overlapping pixel of blocks. Wu and Tsai embedded data

with the range size i.e. shown in Table I. This techniques ability is to refuse analysis attack. Based on PVD method, many papers improved it. PVD approach now mostly proposed with different method for better image quality and embedding capacity.

Wu et al. in 2005 proposed PVD for improving hiding capacity. For hiding data, this is a combination of PVD and LSB substitution. Least significant bit method is very easy and widely used method in steganography. That is why this research also called L-PVD. LSB substitution method applied for smooth and edge area and PVD method applied for embedding capacity at high level amount [18].

Yang et al. [20] has also improved PVD approach in this paper. He improves embedding capacity of image. In this approach AdvPVD adjacent pixel value differencing used for calculate difference between in an adjacent pixel pair. AdvPVD divided into three levels i) low level ii) middle level and iii) high level.

Chin-Feng Lee (2016) [15] have discussed recent pixel value differencing (PVD) based methods. PVD method improved image quality and embedding capacity. This paper provides an easy way to produce a more imperceptible result. Wu and Tsai proposed PVD method in 2013. Basically PVD method increases PSNR value. PVD partitions cover image into different blocks. Every block of image can contain adjacent value.

Mostly PVD based proposed approaches suffer from two major issues:-

I. First is "fall off Boundary Problem".
II. Second is "Low Hiding Capacity".

Now we improve these major issues and summarized into following aspects;

I. An Image Steganography uses benefit of PVD and modulo operation for improving the image quality.
II. For using more consecutive pixels, this proposed approach increases high hiding capacity and first three stego-pixels to be hiding by secret data.
III. End the last avoid fall off boundary problem (FOBP) by using the pixel readjustment process.

Paper work are arranged as follows. Section II introduces illustration of PVD approach related proposed work by WU and Tsai [18]. Section III shows the FOBP issues of Khodaei and Faez's [4] proposed approach with example. Section IV discussed example proposed work by Sahu and Swain [12]. Section V and VI shows this paper proposed work based on PVD and modulo operation and gives an example for the proposed approach. The result and comparisons of this proposed approach to shows the efficiency in Section VII. Section VIII gives conclusion according to this paper work.

II. AN ILLUSTRATION OF PVD APPROACH [18]

Now we show PVD approaches proposed by Wu and Tsai [18] by example and also show range table. In this proposed work, original image is divided into non-consecutive two pixels of block. In this section, embedded and extraction algorithm steps followed in this example that is explained below:-

Step 1: g_1 and g_2 be the two pixels of an original image. Let g_1=80 and g_2 =118.

Step 2: Find'd' be the difference value of two pixels is d= 38€R3 and L_j=32 and U_j=63. The values of R3 are given in range table shown in Table I.

Step 3: 11111_2 are the Secret bits to be hidden in this block n=5 bits.

Step 4: New difference value $d_{new} = dec_n + L_j = 63$, where $dec_n = 31$ and L_j=32.

Step 5: Obtain the difference value 'r' between new and original image value, r=$\left| d_{new} - d \right| = \left| 63 - 38 \right| = 25$.

Step 6: Stego-pixels value is $g'_1 = 68$ and g'_2=131.

Step 7: The difference value d_s at receiver side is $d_s = |68 - 131| = 63€R4$, now obtain s=$|d_s - L_j| = |63 - 32| = 31$.

Step 8: Five binary bit11111_2. This is the extracted bits.

TABLE I
WU AND TSAI RANGE TABLE [18]

Range Rj=[Lj, Uj]	R1=[0,7]	R2=[8, 15]	R3=[16,31]	R4=[32, 63]	R5=[64, 127]	R6=[128, 255]
Capacity, n	3	3	4	5	6	7

III. AN EXAMPLE OF KHODAEI AND FAEZ'S [4]

This proposed approach shows example based on LSB substitution and Pixel value differencing (PVD). In this approach to hide the secret bit inside three consecutive pixel blocks. Original image divided into 1*3 non-overlapping pixels. An embedding and extraction procedures of this approach are shown below.

Step 1: Let g_l , g_c and g_r be the three pixels of a block. g_c Consider the reference pixel of the block. Let $g_l = 255,\ g_c = 255$ and $g_r = 255$.

Step 2: Assume 111100111_2 is secret binary bit of data. After applying k=3 bit LSB substitution on g_c, the value $g'_c = 255$.

Step 3: Consider dec_1 and dec_2 is the decimal value of the k bit LSB substitution of g_c and g'_c respectively. Obtain $dec_1 = 1$ and $dec_2 = 7$. Compute difference between dec_1 and dec_2 as d=$|dec_1 - dec_2|$=$|7 - 7| = 0$.

Step 4: Optimal value of $g'_c = 255$ and difference value $d_1 = 0$ and $d_r = 0$.

Step 5: New difference value $d'_1 = 4$ and $d'_r = 0$. The difference values are considered from the range table as shown in Table II.

Step 6: New value for g_l and g_r as $g_l'' = 251$ and $g_l''' = 259$, $g_r'' = 248$ and $g_r''' = 262$.

Step 7: Stego-pixels $g'_l = 259$ and $g'_r = 262$. Both values are goes above the grayscale range of 0 to 255. So fall off boundary problem exist in this approaches.

TABLE II
KHODAEI AND FAEZ RANGE TABLE [4]

Range Rj=[Lj, Uj]	[0, 7]	[0, 7]	[16, 31]	[32, 63]	[64, 255]
Capacity, n	3	3	3	4	4

IV. AN EXAMPLE OF SAHU AND SWAIN [12]

In this section, we also discuss example of sahu and swain [12] uses PVD approach and modulus function (MF). In this proposed work, original image divided into 1*4 pixel blocks. The step by step example describe according to embedding and extraction algorithm steps.

Step 1: Consider the two consecutive pixels are g_i and g_o, i.e. i=1 to 4.

Step 2: Obtain the difference value of two pixels di=$|\ g_i - \ g_o|$ i.e. i= 1 to 4.

Step 3: According to Table III, di value will take k-bit of data. Secret binary bits convert into decimal value is si. Calculate the new difference value d'i= Lj+si, for i=1 to 4.

Step 4: Now calculated new value of $g_i{}'$ =|go-di'|=169 and $g_i{}''$ =|go+di'|=239.

Step 5: Obtain $g_i *$ for i=1 to 4 i.e. g1*=169, g2*=139, g3*=139, g4*=126. The stego-pixel $g_o *= 205$ computed.

Step 6: The final stego-pixels of the block are g1*=170, g2*=139, g3*=139, g4*=127 and $g_o *= 205$.

Step 7: The differences are d1*=35, d2*=66, d3*=66 and d4*=78.

Step 8: According to difference values, the decimal value for hidden secret data is s1=3, s2=2, s3=2, s4=14 and s_d =5.

Step 9: The extracted binary bits are 0011001000101110101_2

TABLE III
SAHU AND SWAIN RANGE TABLE [12]

Range Rj=[Lj, Uj]	[0, 7]	[8, 15]	[16, 31]	[32, 63]	[64, 255]
Capacity, n	+1	+1	+1	-1	-2

V. THE PROPOSED APPROACH

In this proposed algorithm, we work on Pixel Value Differencing (PVD) and Modulus Operation (MO), PVD and MO improves the image quality measure parameters like Peak Signal to Noise Ratio (PSNR), hiding capacity, Mean Square Error (MSE) etc. In this technique, security features are more reliable as compare to other steganography techniques. It also provides security using Pixel differencing modulo operation (PDMO). In this technique, original image partition into four consecutive non-overlapping pixels of the blocks. Separated pixels are embedding performed in two steps. In first step, pixel differencing modulo operation improve data hiding capacity. Starting three pixels consider for embedding using PVD and MO. In second step, Average pixel value differencing using for readjustment of stego-images. The main aim of this proposed work is that improving average approach and hiding capacity. Originals image divided into blocks such as P_1, P_2, P_c & P_3. P_1, P_2 and Pc used for utilization secret data and P3 used for embed secret data.

In this technique PSNR value increases and MSE value decreases. It also avoid fall off boundary pixels (FOBP). Modulo operation (MO) improve the embedding rate, PVD improve the hiding capacity, Average pixel value differencing (APVD) readjust the stego image pixels. This paper improving image quality and hiding capacity as compares to other steganography techniques. The next subsection shows embedding algorithm and extracting algorithm.

P_1	P_2	P_c	P_3

Fig. 1 Original Image

A. Embedding Algorithm

The embedding algorithm performed with four consecutive pixels of original image. The embedding algorithm performs firstly Pixel value differencing (PVD), modulo operation (MO) and then Average pixel value differencing readjustment (APVD). Initially first three pixels i.e. P_1, P_2 (left pixel) and Pc (center pixel) are utilize for embed secret data. Average of the two stego-pixels from PDMO is obtained. PVD apply for average of the pixel and P_3 pixel of the block use for embedding secret data. We will describe an embedding steps of this dissertation proposed scheme. Embedding algorithm consist two phases. We summarize the process step-by-step.

Process 1: Pixel difference modulo operation (PDMO)

Step 1: Consider Pi and Pc are the consecutive pixels of a block. For i=1, 2

Step 2:Let's'd is the difference between Pi and Pc. Consider (P_1, P_2) represent by 'Pi' and 'Pc' represent center pixel. Where i=1, 2, 3…..so on

d=|Pi-Pc|, i =1, 2, 3. Eq. (1)

Step 3: Consider t_l, t_2 and t_3 are the three number of secret data bits to be embedded on the pixels P_1, P_2 and Pc. Using the difference value d, find t_l, t_2 and t_3 as t_l = t, t_2 = t and t_3=t bits.

Step 4: Compute the remainders rm1, rm2 and rm3 using Eq. (2), (3) and (4).

$$r\ m1=\begin{cases}\text{P1 mod 8,if d}\in\text{R1}\\ \text{P1 mod 16,if d}\in\text{R2}\\ \text{P1 mod 32,if d}\in\text{R3}\end{cases}\qquad \text{Eq. (2)}$$

$$r\ m2=\begin{cases}\text{P2 mod 8,if d}\in\text{R1}\\ \text{P2mod 16,if d}\in\text{R2}\\ \text{P2 mod 32,if d}\in\text{R3}\end{cases}\qquad \text{Eq. (3)}$$

$$r\ m3=\begin{cases}\text{Pc mod 8,if d}\in\text{R1}\\ \text{Pc mod 16,if d}\in\text{R2}\\ \text{Pc mod 32,if d}\in\text{R3}\end{cases}\qquad \text{Eq. (4)}$$

Step 5: Let d1, d2 and d3 be the decimal value of t1, t2 and t3 bits of secret data. Now obtained the difference value dv1, dv2, dv3, dv4, dv5 and dv6 using Eq. (5).

dv1=rm1-d1, dv2=d1-rm1, dv3=rm2-d2, dv4=d2-rm2, dv5=rm3-d3 and dv6=d3-rm3 Eq. (5)

Step 6: Now calculate modified pixels P_1°, P_2° and Pc° using Eq. (6), (7) and (8).

P_1'=

$$\begin{cases} P1, if\ rm1 = d1\\ P1 - dv1,\ if\ rm1 < d1\ and\ |dv1| < 2^{t-1}\\ P1 + dv2,\ if\ rm1 > d1\ and\ |dv2| < 2^{t-1}\\ P1 - dv3,\ \ if\ rm1 < d1\ |dv3| < 2^{t-1}\\ P1 - e, if\ rm1 < d1\ and\ |dv1| > 2^{t-1} where\ e = 2^t + dv1\\ P1 + e, if\ rm1 > d1\ and\ |dv2| > 2^{t-1} where\ e = 2^t + dv2 \end{cases}$$

Eq. (6)

P_2'=

$$\begin{cases} P2, if\ rm2 = d2\\ P2 - dv1,\ if\ rm2 < d2\ and\ |dv1| < 2^{t-1}\\ P2 + dv2,\ if\ rm2 > d2\ and\ |dv2| < 2^{t-1}\\ P2 - dv3,\ \ if\ rm2 < d2\ |dv3| < 2^{t-1}\\ P2 - e, if\ rm2 < d2\ and\ |dv3| > 2^{t-1} where\ e = 2^t + dv3\\ P2 + e, if\ rm2 > d2\ and\ |dv4| > 2^{t-1} where\ e = 2^t + dv4 \end{cases}$$

Eq. (7)

Pc'=

$$\begin{cases} Pc, if\ rm3 = d3\\ Pc - dv1,\ if\ rm3 < d3\ and\ |dv1| < 2^{t-1}\\ Pc + dv2,\ if\ rm3 > d3\ and\ |dv2| < 2^{t-1}\\ Pc - dv3,\ \ if\ rm3 < d3\ |dv3| < 2^{t-1}\\ Pc - e, if\ rm3 < d1\ and\ |dv5| > 2^{t-1} where\ e = 2^t + dv5\\ Pc + e, if\ rm3 > d1\ and\ |dv6| > 2^{t-1} where\ e = 2^t + dv6 \end{cases}$$

Eq. (8)

Step 7: Find d' new difference value. Apply Eq. (9)(d∈R1, d∈ $R2\ and\ d \in R3$) for obtained the stego-pixel pair (P_1*, P_2* and Pc*).

(P_1*, P_2*, Pc*)=

$$\begin{cases} (P1', P2', Pc'), if\ d' \in R1 \\ (P1' - 2^t, P2' + 2^t, Pc' - 2^t), if\ d' \in R2\ and\ P1', Pc' \geq P2' \\ (P1' + 2^t, P2' - 2^t, Pc' + 2^t), if\ d' \in R2\ and\ P1', P2' < Pc' \end{cases}$$

Eq. (9)

(P1*, P2*, Pc*)=

$$\begin{cases} (P1', P2', Pc'), if\ d' \in R2 \\ (P1' + 2^t, P2' - 2^t, Pc' + 2^t), if\ d' \in R1\ and\ P1', Pc' \geq P2' \\ (P1' - 2^t,\ P2' + 2^t, Pc' + 2^t), if\ d' \in R1\ and\ P1', P2' < Pc' \end{cases}$$

Eq. (10)

Step 8: If P_1*, P_2* and Pc* suffer from FOBP then apply Eq. (11)

(P1*, P2*, Pc*)=

$$\begin{cases} (P1 * +2^t, P2 * -2^t, Pc * +2^t), if\ P1 *, P2 * \ and\ Pc * < 0 \\ (P1 * -2^t, P2 * +2^t, Pc * -2^t), if\ P1 *, P2 * \ and\ Pc * > 255 \end{cases}$$

Eq. (11)

Step 9: The stego-pixels P1*, P2* and Pc*.

Process 2: Average Pixel Value Differencing.

Step 1: This process calculate average of first two pixel and third pixels P1*, P2* and Pc, g_{avg} is obtained using Eq. (12)

$$\mathrm{g_{avg}} = \frac{\lfloor (\mathrm{P1}{*} + \mathrm{P2}{*} + \mathrm{Pc}{*}) \rfloor}{3} \qquad \text{Eq. (12)}$$

Step 2: Now apply PVD to g_{avg} and P3. After applying PVD to g'_{avg} and P3' is modified.

Step 3: Compute difference value d_{avg} between g_{avg} and g'_{avg} using Eq. (13)

$$\mathrm{d_{avg}} = |\mathrm{g_{avg}} - \mathrm{g'_{avg}}| \qquad \text{Eq. (13)}$$

Step 4: Now calculate $g *_{avg}$ and P3* using Eq. (14)

$$g *_{avg} = g'_{avg} + d_{avg}, \mathrm{P3^{*}= P3' } + d_{avg} \qquad \text{Eq. (14)}$$

Step 5: Step 6 and 7 execute pixels for overflow and underflow.

Step 6: Overflow gets the largest pixel value lie 255 and calculate $\mathrm{d_{overflow}}$ difference value using Eq. (15), for max ($\mathrm{g} *_{\mathrm{avg}}$, P3*) indicate maximum value between $\mathrm{g} *_{\mathrm{avg}}$ and P3*.

$$\mathrm{d_{overflow}} = \max (\mathrm{g} *_{\mathrm{avg}}\ and\ \mathrm{P3^*}) - 255 \qquad \text{Eq. (15)}$$

Now readjust the pixels $\mathrm{g} *_{\mathrm{avg}}$ and $\mathrm{P3} *$ using Eq. (16)

$$\mathrm{g} *_{\mathrm{avg}} = \mathrm{g} *_{\mathrm{avg}} - \mathrm{d_{overflow}}, \mathrm{P3} *= \mathrm{P3} * - \mathrm{d_{overflow}}$$

Eq. (16)

Step 7: Underflow gets the smallest pixel value lie less than 0. Calculate the difference value $\mathrm{d_{underflow}}$ using Eq. (17), for min ($\mathrm{g} *_{\mathrm{avg}}$, P3*) indicate the minimum value between $\mathrm{g} *_{\mathrm{avg}}$ and P3*.

$$\mathrm{d_{underflow}} = \min (\mathrm{g} *_{\mathrm{avg}}\ \text{and}\ \mathrm{P3} *) - 0$$

Eq. (17)

Now readjust the pixel value $\mathrm{g} *_{\mathrm{avg}}$ and $\mathrm{P3} *$ using Eq. (18)

$$\mathrm{g} *_{\mathrm{avg}} = \mathrm{g} *_{\mathrm{avg}} - \mathrm{d_{underflow}}, \mathrm{P3} *= \mathrm{P3} * - \mathrm{d_{underflow}}$$

Eq. (18)

Step 8: Now stego-pixels value is P1*, P2*, Pc* and P3*.

Step 9: Now embedding algorithm is completed.

Range table of this proposed approach shown in Table IV.

TABLE IV
RANGE TABLE OF THIS PROPOSED APPROACH

Range (Rj)= (Lj, Uj)	R1={0, 15 }	R2={16, 31}	R3={32, 255}
Capacity, t	Log2(Uj-Lj+1)-2	Log2(Uj-Lj+1)-3	Log2(Uj-Lj+1)-4

B. Extraction Algorithm

Extraction algorithm is the inverse of an embedding algorithm. For extract secret data from images is done by this technique. Both side sender and receiver must be same key for extract secret data. In this paper, we will describe an extracting algorithm process step-by-step as follows.

P_1*	P_2*	Pc*	P_3*

Fig. 2 Stego-pixel Block

Step 1: Let P1*, P2*, Pc* and P3* be the stego pixels of a block, as shown in Fig.2.

Step 2: Now calculate $'\mathrm{d_s}'$ difference value using Eq. (19).

$$\mathrm{d_s} = \mathrm{Pi} * - \mathrm{Pc} *, \mathrm{for\ i} = 1,2 \qquad \text{Eq. (19)}$$

Now calculate remainder values $\mathrm{r_{m1}} *, \mathrm{r_{m2}} *$ and $\mathrm{r_{m3}} *$ using Eq. (20), (21) and (22).

$$\mathrm{r_{m1*}} = \begin{cases} \mathrm{P1\ mod\ 8, if\ d \in R1} \\ \mathrm{P1\ mod\ 16, if\ d \in R2} \\ \mathrm{P1\ mod\ 32, if\ d \in R3} \end{cases} \qquad \text{Eq. (20)}$$

$$r_{m2*} = \begin{cases} P2 \bmod 8, \text{if } d \in R1 \\ P2 \bmod 16, \text{if } d \in R2 \\ P2 \bmod 32, \text{if } d \in R3 \end{cases} \qquad \text{Eq. (21)}$$

$$r_{m3*} = \begin{cases} P3 \bmod 8, \text{if } d \in R1 \\ P3 \bmod 16, \text{if } d \in R2 \\ P3 \bmod 32, \text{if } d \in R3 \end{cases} \qquad \text{Eq. (22)}$$

Step 3: Now calculate average of the stego-pixels $g*_{avg}$ can be found using Eq. (23)

$$g *_{avg} = \frac{\lfloor (P1* + P2* + Pc*) \rfloor}{3} \qquad \text{Eq. (23)}$$

Step 4: Now apply pixel value differencing approach for extraction process to obtain the secret data bits from $g*_{avg}$ and P3*.
Step 5: Then finally extracted secret data bits using step 3 and step 5.
Step 6: Extraction process are completed.

VI. AN EXAMPLE OF THE PROPOSED APPROACH

A. Embedding Steps

Step 1: Consider P1=128, P2=126, Pc=124 and P3=122 are three original pixels.
Step 2: Calculate the difference value d is 4 and 2 using eq. (1).
Step 3: Assume $(110010011)_2$ be the secret binary bits (d€R1). Number of bits to be embedded t1, t2 and t3 in P1, P2 and Pc is 12, 9 and 1.
Step 4: The remainders value rm1=7, rm2=6 and rm3=5 using eq. (2), (3) and (4).
Step 5: The decimal values for t1, t2, and t3 bits of secret data are d1=6, d2=4 and d3=2. The difference value dv1, dv2, dv3, dv4, dv5 and dv6 are getting through the eq. (5) as 1, -1, 2, -2, 3 and -3.
Step 6: The modified pixel values P1'=106, P2'=123 and Pc'=121are found from eq. (6), (7) and (8).
Step 7: Now new difference value di'=4 and 2 using eq. (10). Then the stego-pixel pair P1*=106, P2*=123 and Pc*=121.
Step 8: Average of modified pixel gavg=116 after apply PVD.
Step 9: After applying PVD, the modified pixels are g'avg= 122 and P3'=119.
Step 10: Difference value davg is 5 through the eq. (13).
Step 11: Obtained g*avg=116 and P3*=122 using eq. (14).
Step 12: At last no overflow and underflow pixel in this block, the final stego-pixel values are P1*=106, P2*=123, Pc*=121 and P3*=119.
Step 13: Embedding process are completed.

B. Extracting Steps

Step 1: Let P1*=106, P2*=123, Pc*=121 and P3*=119 are the stego-image pixels.
Step 2: Difference value ds=15and 2. Calculate remainder value rm1*, rm2* and rmc* as 8, 6 and 2 respectively.
Step 3: Now difference value d€R1, represent 3 bits respectively. The extracted bits is 1100110.
Step 4: Average of the stego-pixels is g*avg=116.
Step 5: Now apply the PVD extraction process to g*avg and P3* and extract the secret bits 0110. After concatenating 0110 with 1100 gives 1100110_2.
Step 6: Now extracting phases is completed.

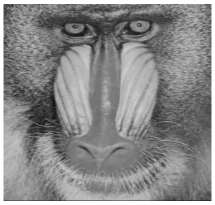
VII. RESULT AND CONCLUSION

In this proposed approach, original images are considered from USC-SIPI [25], CVonline [26]. Original images and stego-images are shown in Fig 3 and Fig. 4. PSNR, capacity, bit per pixel (BPP) and FOBP counts for the proposed approach in Table IV. The PSNR values calculate the stego-image quality and high PSNR value recommended best and good image quality. PSNR value computed using Eq. (27).

$$PSNR = 10 log_{10} \frac{255*255}{\frac{1}{m*n} \sum_{i=1}^{m} \sum_{j=1}^{n} (Xij - Yij)^2}$$

Eq. (27)

Where Xij= Pixel of Cover image and Yij= Pixel of stego image at ith and jth coordinates respectively.
The most important advantage of this proposed work is that we can not suffer from fall off boundary problem.



a) Baboon

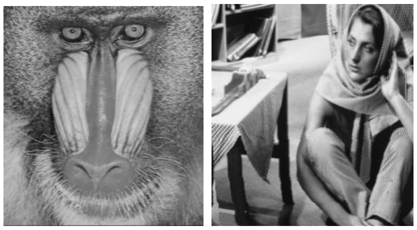
b) Barbra

c) Bridge

d) boat

e) Couple f) Girlface

Fig. 3 Original Image



a) Baboon b) Barbra

c) Boat d) Bridge

e) Couple f) Girlface

Fig. 4 Stego Image

TABLE V
RESULT OF THE PROPOSED APPROACH, WU AND TSAI, KHODAEI AND FAEZ

	Proposed Approach				Wu and Tsai				Khodaei and Faez			
	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP	PSNR	Capacity	BPP	FOBP
Baboon	42.01	835,055	3.16	0	38.01	441,098	1.68	0	36.27	801,902	3.06	0
Barbra	47.99	840,032	3.30	0	37.04	438,949	1.67	3009	30.03	819,540	3.13	0
Boat	50.33	849,001	3.12	0	39.03	421,750	1.61	109	37.11	795,480	3.03	0

VIII. CONCLUSION

This proposed work using MATLAB R2019b. In this approach we improve the hiding capacity of data based on Pixel Value Differencing and Modulo Operation.

Data embedding is done by PDMO and APVD process. PVD and MO consider three consecutive pixels for embed data then found average of starting three stego-image pixels. According to proposed approach, PSNR and capacity are 50.33 and 849,001 bits. It also avoid fall off boundary problems.

Future works on extending proposed approach and more than four consecutive pixels improve the quality and hiding capacity of image without any changes in an image quality. In future, we extending in the direction of reversible data hiding technique (RDH).

REFERENCES

[1] “A Review Paper on Cryptography” Abdalbasit Mohammed Qadir Software Engineering Department Firat University Elazig, Turkey, Nurhayat Varol TBMYO

Firat University Elazig, Turkey

[2]https://economictimes.indiatimes.com/definition/cryptography.

[3] Manjit Thapa, Sandeep KumarSood” On Secure Digital Image Watermarking Techniques,2011

[4] Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image processing*, *6*(6), 677-686.

[5] Shoemaker, ―Hidden bits: A survey of techniques for digital watermarking‖, Independent study, EER 290, spring 2002.

[6] Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," Expert System with Applications, vol. 42, pp. 8198-8211, 2015.

[7] A.Nag!, S. Biswas*, D. Sarkar*, P.P. Sarkar*” A novel technique for image steganography based on Block-DCT and Huffman Encoding”.

[8] International Refereed Journal of Engineering and Science (IRJES) ISSN (Online) 2319-183X, (Print) 2319-1821 Volume 6, Issue 1 (January 2017), PP.68-71 Namrata Singh Computer Science and Engineering ABES Engineering College, Ghaziabad A.K.T.U” Survey Paper on Steganography”, 2017.

[9] https://ieeexplore.ieee.org/document/6496564

[10] Chung-Ming Wang, Nan-I-Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, A High Quality Steganographic Method with pixel value differencing and modulus function, The Jurnal of System and Software (2008).

[11] “Digital Image Steganography Using LSB Substitution, PVD, and EMD” Anita Pradhan,[1] K. Raja Sekhar,[1] and Gandharba Swain[1]

[12] “A Review on LSB Substitution and PVD Based Image Steganography Techniques” Aditya Kumar Sahu*, Gandharba Swain.

[13] “SURVEY ON DIFFERENT METHODS OF IMAGE STEGANOGRAPHY” B.Deekshitha1 , Gnanamanjari.S2 , Chaithanya.S3(2017).

[14] “Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security” Rojalia , Ida Sri Rejeki Siahaanb , Benfano Soewito(2017).

[15] “The Study of Steganographic Algorithms Based on Pixel Value Difference” Chin-Feng Lee*,1,Jau-Ji Shen2 , Kuan-Ting Lin3(2016).

[16] “PVD Based Steganography on Scrambled RGB Cover Images with Pixel Indicator” V. Thanikaiselvan, S.Subashanthini and Rengarajan Amirtharajan (2014).

[17] Data Hiding Using Steganography: A Review Nishigandha P. Mangle1, Prof. Sanjay S. Dhopte2(2012).

[18] H.C. Wu, N.I. Wu, C.S. Tsai, and M. S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” Proc. Inst. Elect. Eng., Vis. Images Signal Processing, vol. 152, no. 5, pp. 611–615(2005).

[19] K.C. Chang, P. S. Huang and C. P. Chang, “Adaptive image steganographic scheme based on tri-way pixel-value differencing,” Systems, Man and Cybernetics, IEEE, pages 1165–1170(2007).

[20] C.H. Yang, C.Y. Weng, S.J. Wang and H.M. Sun, “Adaptive data hiding in edge areas of images with spatial LSB domain systems”. IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, p. 488–497(2008).

[21] C.M. Wang, N.I. Wu, C.S. Tsai and M. S. Hwang, “A high quality steganography method with pixel-value differencing and modulus function”, J. Syst. Softw., vol. 81, pp. 150–158(2008).

[22] S.Y. Shen, L.H. Huang, “A data hiding scheme using pixel value differencing and improving exploiting modification directions” Computers & Security., vol.48, pp. 131 (2015).

[23] Gandharba Swain, Digital Image Steganography using Nine-Pixel Differencing and Modified LSB Substitution, Indian Journal of Science and Technology, Vol 7(9), 1444–1450 (2014)

[24] Bismita Chaudhary “A Novel Steganalysis Method based on Histogram Analysis”Electrical Engineering(2015).

[25]http://sipi.usc.edu/database/database.php?volume=misc.

[26]http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm.