Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding

Marwa E. Saleh *marwa.emadeldeen@gmail.com*
Faculty of Computers and Information,
Dept. of Computer Science
Minia University
Minia, Egypt

Abdelmgeid A. Aly *abdelmgeid@yahoo.com*
Faculty of Science,
Dept. of Computer Science
Minia University
Minia, Egypt

Fatma A. Omara *f.omara@fci-cu.edu.eg*
Faculty of Computers and Information,
Dept. of Computer Science
Cairo University
Cairo, Egypt

Abstract

Information hiding could be done using steganography and watermarking. According to steganography, secret information is embedded in carriers such as image, sound, video in such a way that it couldn't be detected. On the other hand, watermarking is used for copyright preservation. By using images as carriers in steganography, there are many methods have been proposed for image steganography. Pixel Value Differencing (PVD) is one of basic methods of image steganography, in which the difference between pixels are used to hide the secret message. In this paper, a new image steganography enhancement method for the Pixel Value Difference (PVD) method has been proposed. The principle of the proposed method is based on using Mobile Phone Keypad (MPK) Coding technique and Modified Substitute Last Digit In Pixel by using Mobile Phone Keypad (MSLDIP-MPK) method. The main enhancement component of the proposed method is called (PVD-MPK). Due to this enhancement component, Maximum Hiding Capacity (MHC) of the cover image is enlarged, and the stego image quality or Peak Signal-to-Noise Ratio (PSNR) values is enhanced.

Keywords: Image Steganography**,** Pixel Value Difference (PVD), Peak signal-to-Noise Ratio (PSNR)**,** Mean Square Error (MSE).

1. INTRODUCTION

The most powerful and common approaches to countering the threats to network / information security are encryption and steganography. Encryption based on applying number of substitutions, and transpositions to convert the text into cipher text. This process of converting is called Cryptography [1]. Steganography is a form of covert communication in which a secret message is camouflaged within a carrier message. Steganography is considered the art and science of invisible communication. This is accomplished by hiding information in other information. The word Steganography is derived from the Greek words “stegos” meaning “cover” and, “grafia” meaning “writing” defining it as “covered writing” [2].

There are two common techniques of embedding in image steganography; spatial domain embedding in where messages are inserted into LSBs such as LSB of pixels, and Transform domain embedding in where a message is embedded by modifying frequency coefficients of the

cover image (the resulted image is called the stego-image) [3]. The spatial domain embedding is considered in this paper

Least Significant Bit Substitution (LSB) is the most commonly used stenographic technique. The basic concept of Least Significant Bit Substitution includes the embedding of the secret data at the bits which having minimum weighting such that it will not affect the value of original pixel. Although LSB insertion is simple and good for steganography, but its major drawback is the ease of extraction [3, 4].

On the other hand, image steganography system is comprised two algorithms, one for embedding and one for extraction. The embedding process is concerned with hiding a secret message within a cover media (cover image), which is the most carefully constructed process. The main issue is to grantee that the secret message will not be unnoticed if a third party tries to intercept the cover media (cover image). The extraction process is simply because it is the inverse of the embedding process, where the secret message is revealed at the end [5].

The basic model of steganography is shown in Figure (1). According to Figure (1), steganography process consists of carrier, message and password. Carrier is also known as cover-object or cover-image, in which message is embedded. The message can be any type of data (plain text, cipher text or other image) that the sender wishes to remain confidential. Password is known as stego-key, which ensures that only recipient who has the decoding key will be able to extract the message from a stego-object. Finally, the cover-object with the secretly embedded message is called the stego-object or stego-image [5].

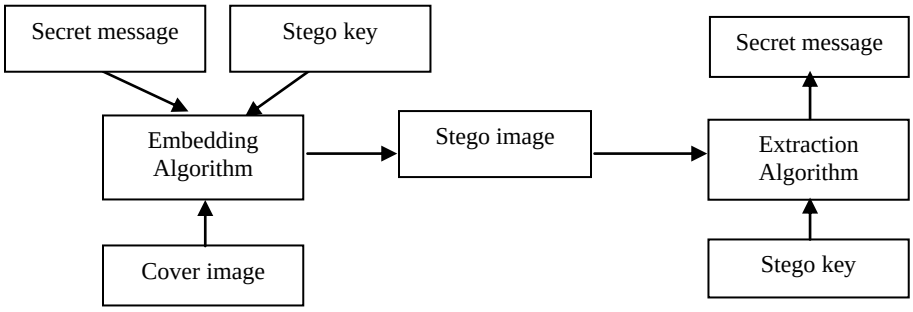

FIGURE 1: The Basic Model of Steganography.

Actually, carriers could be images, audio, video, or text files, but digital images are the most commonly used because of these reasons [6]:

1. Natural image data can be modified slightly without leading to visible artefacts (if the colour of a few pixels is shifted slightly in one direction or another, it is likely to go unnoticed).
2. These types of files are inherently anonymous nature on the internet.
3. It contains a significant amount of data, enabling high secret communication rates.

The main objectives of a steganography technique are [7]:

1. Capacity; the amount of information that can be hidden in the cover medium.
2. Security; related to the eavesdropper's inability to extract hidden information.
3. Robustness; the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.
4. Imperceptibility; referred to the perceptual difference between the cover and original signal.

One of the performance issues should be measured for image distortion due to embedding is the peak signal-to noise ratio (PSNR), which is used to evaluate the quality of the stego-image. The PSNR is given by the following formula [3]:

$$PSNR=10 \log_{10} (C^2_{max}/MSE)$$

Where, C max holds the maximum value in the image that is 255 and MSE is the mean square error, which is given by:

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})$$

Mean Square Error (MSE) is used to quantify the difference between the initial and the distorted or noisy image. X and Y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the generated stego-image and C_{xy} is the cover image [3].

The rest of this paper is organized as follows; related work will be discussed in section 2, the proposed method will be proposed in section 3, experimental results of proposed method will be given in section 4, finally section 5 conclusions and future work of the paper.

2. RELATED WORK

An image is an array of square pixels (picture elements) arranged in columns and rows. Today digital images are most widely used for hiding the secret messages. Capacity with good image quality of stego image is very important aspect [8]. The LSB-based methods directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the differences between adjacent pixels. The differences between adjacent pixels methods produce a more imperceptible result than those obtained from simple least-significant-bit substitution methods. In general, the hiding capacity of the two consecutive pixels depends on the difference value. In other words, the smoother area is, the less secret data can be hidden; on the contrary, the more edges an area has, the more secret data can be embedded.

Wu et al [9] have presented a novel steganographic method, which combined pixel-value differencing and LSB substitution, where the smooth areas, and the secret data are hidden into the cover image by LSB method hide 6-bit secret data (3bit for each pixel) while using the PVD method in the edged areas.

In [10], Wang et al have improved the stego-image quality by adjusting the remainder of the two consecutive pixels instead of the difference value to record the information of the secret data which gains more flexibility, capable of deriving the optimal remainder of the two pixels at the least distortion. The hiding effect that appears in the stego-image when Wu and Tsai's scheme is used to hide the secret data can be significantly decreased by this optimal embedding algorithm. Experimental results show the scheme has a much better performance than Wu and Tsai's scheme in terms of stego-image quality.

Also, Yang et al [11] have proposed an adaptive LSB steganographic method using the difference value of two consecutive pixels to distinguish between edge areas and smooth areas. Pixels located in edge areas are embedded by k-bit LSB substitution method with a larger value of than that of the pixels located in smooth areas.

A novel steganographic approach using tri-way pixel-value differencing (TPVD) has been proposed in [12]. To upgrade the hiding capacity of original PVD method referring to only one direction, three different directional edges are considered and adopted to design the scheme of tri-way pixel-value differencing. In addition, to reduce the quality distortion of stego-image brought from setting larger embedding capacity, an optimal approach of selecting the reference point and adaptive rules is presented. By using three different directional edges more secret data can be hidden into the cover image than the PVD method. Also, the optimal selection approach for the reference point with adaptive used rules to reduce the quality distortion of the stego-image.

A variation of existing PVD method called as Edged PVD has been suggested to increase the embedding capacity of the stego image [13]. The proposed method involves examining 2X2 pixel group and finding the direction of max slope. This direction is selected for embedding the secret message. In this case, since the maximum slope is selected, the capacity is increased by as much as 6- 7% at the cost of slightly increasing in MSE and AFCPV. The embedding and retrieval of secret message are the same as the original PVD method. However this does not affect the perceptibility and stego image appears to be as good as the original image.

A steganographic method has been presented for hiding data in the images [14]. The MLSB and MF&PVD methods are used in this method. According to this method, the capacity of the hidden secret data and stego image quality have been improved. A small difference value between two pixels of each block is located on a smooth area and the large differences are located on the edge areas. In the smooth areas, the secret data was hidden into the cover image by MLSB method for achieving more capacity and better quality, whereas, the MF&PVD method is used in the edge.

The OCTA (STAR) PVD method has been presented to modify the existing TPVD method by considering 3 X 3 pixel pairs instead of 2 X 2 pixel pairs [8]. Due to the number of available pairs for data hiding is to 8 as compared to TPVD's 3, so more data is hidden with better security.

There are three attempts will be used to develop the proposed image steganography method:

In [6] a new image steganography technique called Substitute Last Digit In Pixel or (SLDIP) has been proposed, in which the cover image is divided into non overlapping blocks, and each block contains three pixels only and the secret message is converted into its ASCII code where each character will be represented by three digits only. As an example, if the secret letter is R and the current block contains 255, 200 and 101, R will be hidden by representing in ASCII format and it will equal 082. Then the pixels after substitution will be 250, 208 and 102 instead of 255, 200 and 101. So the last digit only will be substituted. These digits will be used for extraction process, as every three pixels' last digits will represent a byte in the secret message. This SLDIP technique has a very high PSNR values and a very high MHC in which each secret byte can be hidden in only three pixels of the cover images. The SLDIP technique has been modified. According to the modified version of the SLDIP method, it is able to keep the same Maximum Hiding Capacity of the SLDIP Method plus higher PSNR values than SLDIP. In this method the differences between the block are minimized before and after the embedding step and this modification is done by taking two possible values for each substitution and choosing the value that has the smallest difference. By considering the same example, for embedding the secret message R which equals 082 in ASCII, in the first block (255, 200, and 101), instead of (250, 208 and 102), the difference between the original pixel and the substituted pixel in the second pixel will be 8. By using MSLDIP method, the possible value for the substitution will be 208 and 198, and the smallest difference (i.e., 198) will be considered. So, the difference will be 2 instead of 8, this increases the PSNR value of the image.

In [15], Mobile Phone Keypad (MPK) encoding has been proposed that is a way to modify the secret message. It has been found that each character in the mobile phone can be represented by only two digits not three as ASCII encoding. So, the mobile phone character is used to develop a new encoding technique for encoding the secret message with smaller number of digits than ASCII. This method is called MPK (Mobile Phone Keypad) encoding. As an example, by using the mobile phone, the letter a can be typed by pressing the key no.# (2) in the keypad only one time and the letter b can be typed by pressing the key no.# (2) for two times and so on. So, the first step is used to represent the letters from a … z using two numbers, the first key is no.# and the second will be the number of presses on that key. As an example, the letter a will be represented as 2 1 and the letter z will be represented as 9 4 (will be read as nine - four separately) and so on. Also, the MPK method has been used in the modified MSLDIP method [6], and has been called it MSLDIP-MPK method.

Wu and Tsai [16] have presented steganographic scheme that hide a secret message into a gray -valued cover image. For embedding a secret message, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. In each block, a difference value is calculated from the values of the two pixels. If the difference value is large, that means the two pixels are located in an edge areas, and more secret data can be hidden there. On the contrary, if the difference value is small, that means the two pixels are located in a smooth area, and less secret data can be embedded. Then, this difference value is replaced by a new value to embed the value of the secret message. This method produces a more imperceptible result than those obtained from simple least-significant-bit substitution methods. The embedded secret message can be extracted from the resulting stego-image without referencing the original cover image.

3. THE PROPOSED METHOD

An enhancement of the PVD method using Mobile Phone Keypad is proposed, called (PVD-MPK) method. The MSLDIP-MRK algorithm will be combined with the proposed PVD-MPK method, so in the smooth areas we use PVD-MPK to increase the quality, and use MSLDIP-MPK method in the edge areas to increase the capacity. The range [0,255] must be divided into two levels; the 'low-level' (i.e., smooth areas) and 'high-level' (i.e., edge areas) and the range table division is controlled by the users. Anyone who has extracted the secret data from a stego image must use the original division.

3.1 The PVD-MPK Method

The principle of this method is using the digits of MPK encoding instead of bits of secret message to increase the capacity and quality because MPK encoding represents each character by two digits instead of three digits as in ASCII format, and embeds digit in each block in the smooth area. According to the proposed method, range table will be different from the range table in the original PVD. Here, the ranges will be (0-4), (5-9), (10-14), (15-19), (20-24), (25-29) etc. to improve the quality. By using this method, the byte will be hidden in four pixels. The pseudo code of the PVD-MPK method is as follows:

Algorithm: PVD-MPK
Input: Cover Image C, Secret Message M.
Output: StegoImage S.
Steps:

1. Convert each byte from M to MPK format (i.e. two digits for each character).
2. The cover image (C) is divided into non-overlapping blocks, where each block consists of two consecutive pixels.
3. Calculate the difference value di for each block of two consecutive pixels P_i , P_{i+1} ; which is given by (1):
   $$d_i = |p_{i+1} - p_i| \quad (1)$$
4. Find the optimum range R_i for each di where $R_i \in [l_i, u_i]$. Here, l_i and u_i are the lower and upper bound of each range of the range table and $l_i \le d_i \le u_i$.
5. Select one digit (b) from M in MPK format.
6. Calculate the new difference by (2):
   $$d_i` = l_i + b/2 \quad (2)$$
7. Compute the remainder value by (3)
   $$Rem = b \bmod 2 \quad (3)$$
8. Make the difference between p_i and p_{i+1} equal to new difference $d_i`$ by (4)

$$(p`_i, p`_{i+1}) = \begin{cases} \left(p_i + \left\lceil \frac{m}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), \\ \text{if } p_i \geq p_{i+1} \text{ and } d'_i > d_i; \\ \left(p_i - \left\lceil \frac{m}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), \\ \text{if } p_i < p_{i+1} \text{ and } d'_i > d_i; \\ \left(p_i - \left\lceil \frac{m}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), \\ \text{if } p_i \geq p_{i+1} \text{ and } d'_i \leq d_i; \\ \left(p_i + \left\lceil \frac{m}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), \\ \text{if } p_i < p_{i+1} \text{ and } d'_i \leq d_i, \end{cases} \quad (4)$$

The cases in equation (4) adjust the value of pi and p_{i+1} to modify the difference. Where, m is the difference between the original and the new differences (i.e., $m=|d_i - d_i`|$), $p_i$ and $p_{i+1}$ are the first and second pixel in a block before embedding, and $p`_i$ and $p`_{i+1}$ are the first and second pixel in a block after embedding .This equation used in original PVD [16].

9. If Rem equal 1, make p_i odd, else make p_i even.
10. Repeat steps from 3 to 9 until the whole M has been embedded.
11. Convert C back into a layer again to get the StegoImage S.

The used range table is presented in Table 1.

R1∈(0,4)
R2∈(5,9)
R3∈(10,14)
R4∈(15,19)
R5∈(20,24)
.
.
.

TABLE 1: Range Table.

As we explained the main enhancement component of the proposed method is (PVD-MPK) because of two reason; the first it uses digits of MPK encoding instead of bits of secret message, this due to increase capacity because it embeds one digit in each block in the smooth area while the original PVD embeds 3 bits in each block in the smooth area, and the second it uses small ranges, this due to increase quality. .

The reason of using ranges (0-4), (5-9), (10-14), (15-19), (20-24), (25-29) and etc. is that in the original PVD, the width of range is used to compute the number of bits that should be hidden. But by using digits, the width of each range will be equal to the maximum value of digit which is 9(i.e., (0-9), (10-19), (20-29), (30-39), (40-49)… etc.), because when the value of digit is added to the lower bound of the range, the new difference will be in the same range.

Example 1: To illustrate the case of using the ranges (0-9), (10-19), (20-29), (30-39)… etc.

- Assume $p_i = 23$, $p_{i+1} = 42$, and b=0.
- $|d_i| = 19$, so the optimum range $R_2 = (10, 19)$, and PVD-MPK method will be applied.
- b = 0 so $d_i` = 10+0 = 10$.
- m=19 -10=9.
- Applying equation (4), here $p_i < p_{i+1}$, $d_i` < d_i$, so apply the case 4 in (4), and $p_i$ and $p_{i+1}$ will be $p`_i = 28$, $p`_{i+1} = 38$

According to this example, it is found that the change in the first pixel is 5 and in the second pixel is 6. So, we need to decrease these changes to increase the quality of the image. To do this, we need to decrease both the width of each range and the value of the digit. The ranges will be (0-4); (5-9); (10-14) ;(15-19); (20-24); (25-29) etc., the division and remainder are used to decrease the value of digits. In this case, the maximum change in pixel will be 3.

The same example is used to illustrate the improvement when the ranges (0-4); (5-9); (10-14); (15-19); (20-24); (25-29)… etc. is used.

- Assume $p_i = 23$, $p_{i+1} = 42$, and b=0.
- $|d_i|= 19$, so the optimum range $R_4 = (15, 19)$, and PVD_MPK method will be applied.
- b = 0 so d`=15+0=15.
- m=19 -15=4.
- Applying equation (4), here $p_i < p_{i+1}$, $d_i` < d_i$, so apply the case 4 in (4), and $p_i$ and $p_{i+1}$ will be $p`_i$=25, $p`_{i+1}$=40.
- Rem =0, so $p`_i$ must be even and $p`_i$=26, $p`_{i+1}$=41

So, the change in first pixel is 3 instead 5 and in second pixel is 1 instead 6.

3.2 The Embedding Algorithm

Division Div is used to divide between the 'low-level' and 'high-level'. Let, Div = 19. So, the 'low-level' is set to be R1 and R2, R3, R4, and the 'high level' is set to be R5 which are shown in Table 2. The pseudo code of the embedding algorithm is as follows.

Algorithm: Message Embedding Using PVD-MPK and MSLDIP-MPK methods
Input: Cover Image C ; Secret Message M.
Output: StegoImage S.
Steps:

1. Convert each byte from M to MPK format (two digits for each character).
2. The cover image (C) is divided into non-overlapping blocks, where each block consists of two consecutive pixels.
3. Calculate the difference value di for each block of two consecutive pixels P_i , P_{i+1} ; which is given by (1):

$$d_i=|p_{i+1} – p_i| \quad (1)$$

4. Find the optimum range R_i for each di where $R_i \in [l_i, u_i]$. Here, l_i and u_i are the lower and upper bound of each range of the range table and $l_i \le d_i \le u_i$.
5. If R_i belongs to lower level then select one digit from M and make embedding by PVD-MPK method.
   Else if R_i belongs to higher level then select two digits from M and make embedding by MSLDIP-MPK method
6. Repeat steps 3, 4, and 5 until the whole M has been embedded.
7. Convert C back into a layer again to get the StegoImage S.

We note that the less of Div value, the more of using the MSLDIP-MPK method and less of using the proposed PVD-MPK method. So, more the secret data can be embedded because the MSLDIP-MPK method embeds two digits in block, the less of PSNR value, and vice versa. Here the range table is divided to low level and high level as shown in Table 2.

Low level	R1∈(0,4)
	R2∈(5,9)
	R3∈(10,14)
	R4∈(15,19)
High level	R5∈(20,255)

TABLE 2: Range Table.

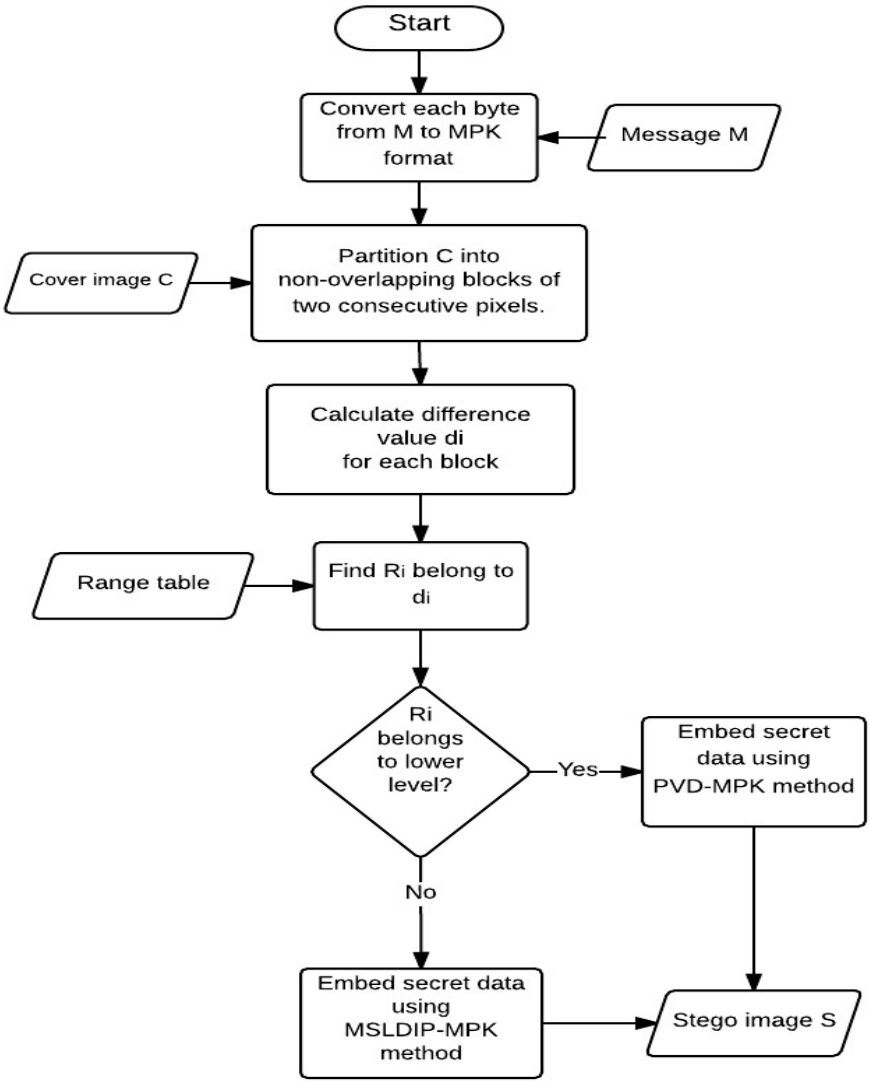

FIGURE 2: The data embedding process.

Example 2: This example illustrates the case when range belong to low level

- Assume $p_i = 101$, $p_{i+1} = 103$, and secret data (message) is 'marwa'.
- After convert message to MPK format will be '6121739121'.
- $|d_i| = 2$, so the optimum range $R_1 = (0, 4)$, and we will apply PVD_MPK.
- b = 6 so d`=0+6/2=3.
- Apply equation (4), here $p_i < p_{i+1}$, d_i `> $d_i$, and m =3-2=1 so apply the case 2 in (4), $p_i$ and $p_{i+1}$ will be $p`_i$ =101 , $p`_{i+1}$ =104.
- Rem =0, so $p`_i$ must be even and $p`_i$ =102, $p`_{i+1}$ =105.

Example 3: This example illustrates the case when range belong to high level

- Assume $p_i = 102$, $p_{i+1} = 66$, and the same secret data (message).
- |di|= 36, so the optimum range is $R_5 = (20, 255)$ and we will apply MSLDIP-MPK.
- The two digits are 1 and 2, so after apply MSLDIP-MPK p_i and p_{i+1} will be $p`_i = 101$, $p`_{i+1}$ =62.

3.3 The Extracting Algorithm

The following Algorithm is executed to recover the original secret data.

Algorithm: Message extracted
Input : StegoImage S.
Output : Secret Message M.
Steps:

1. Partition the Stego-image into non-overlapping blocks of two consecutive pixels,
2. Calculate the difference value $d`_i$ for each block of two consecutive pixels $P`_i$, $P`_{i+1}$ of the stego-image which is given by(5):

$$d`_i = |p`_i - p`_{i+1}| \quad (5)$$

3. Find the R_i belong to $d`_i$ according to the original range table and judge the level of the R_i that depend by using the original set Div value.
4. Extract secret data by using MSLDIP-MPK method if R_i belongs to the high-level, otherwise, carry out the next steps to extract secret data;
    - Subtract li from $d`$ and add the remainder of the first pixel to them, b0 is obtained; the b0 value represents the secret data in decimal number.

$$b_0 = (d_i` - l_i) + p`_i \bmod 2. \quad (6)$$

5. A repeat step 2, 3, 4, and 5 until the whole digits of M has been extracted.
6. Covert each two digit to character by using MPK decoding.

4. EXPERIMENTAL RESULTS

In our experimental environment, we use PC that is installed on windows 7 and equipped with a Genuine Intel(R) Core(TM) 2 Duo CPU 2.20 GHz with 3.0 GB memory. We use MATLAB R2011b and Matlab code to implement the algorithm.

Several experiments with 512 * 512 and 256 * 256 standard gray-scale images are preformed to evaluate our proposed method. Embedding capacity and stego image's visual quality (PSNR) are used to evaluate our proposed image steganography method performance.

Cover image 256*256	Capacity (bytes)	PSNR of method in [13]	PSNR of Proposed method
Baboon	18,616	33.80	41.7789
Lena	13,003	43.56	45.3734
Pepper	16,394	36.91	44.1038

TABLE 3: Comparison between method in [13] with the proposed method and DIV=19.

The results of the comparison study between our proposed method and the method in [13] by using different number of characters (bytes) secret message and 256x 256 cover images (baboon, lena, pepper) are presented in Table 3. According to the comparison results, it is found that our method has more PSNR values than that the method in [13] which means that the stego image quality of our method will be higher than the stego image quality of the method in [13].

Cover image 512*512	Capacity (bytes)	PSNR of method in [14]	PSNR of Proposed method
Baboon	66,397	42.38	42.9366
Lena	66,064	43.77	45.0456
Peppers	65,889	43.11	44.8467
Airplane	65,723	43.96	44.0899
Cameraman	66,198	43.57	45.5351

TABLE 4: Comparison between method in [14] with the proposed method and DIV=19.

TABLE 4 represents the comparative results of our proposed method and the method in [14] using different numbers of characters (bytes) secret message and 512x 512 cover images (baboon, lena, pepper, Airplane, Cameraman). According to the comparative results, it is found that our method has more PSNR values than that the method in [14] which means that the stego image quality of our proposed method will be higher.

Cover Image 512x512	Capacity (bytes)	PSNR of OCTA (STAR) PVD[8]	PSNR of Proposed method
Lena	52.430	41.53	46.1116
Baboon	52.430	39.49	43.8541

TABLE 5: Comparison of paper [8] with the proposed method and DIV=19.

Also, TABLE 5 represents the comparative results of our proposed method and the method in [8] by using different numbers of characters (bytes) secret message and 512x 512 cover images (lena, baboon). According to the comparative results, it is found that our method has more PSNR values than that the method in [8] which means that the stego image quality of our proposed method will be also higher.

Cover Image 512x512	Capacity (bytes)	PSNR of method in [17]	Capacity (bytes)	PSNR of Proposed method
Baboon	57.043	39.2	73.417	42.5196
Boat	52.490	41.0	69.358	44.6589
House	52.572	41.5	66.979	45.4899
Lake	52,662	41.5	72936	43.6962
Lena	50.894	43.4	68.488	44.8864
Peppers	50.815	42.5	69.014	44.6510

TABLE 6: Comparison of paper [17] with the proposed method and DIV=19.

Finally, TABLE 6 represents the comparative results of our proposed method and the method in [17] by using different numbers of characters (bytes) secret message and 512x 512 cover images (baboon, boat, house, lake, lena, peppers). According to the comparative results, it is found that our method has more capacity and more PSNR values than that the method in [17] which means that the MHC and stego image quality of our proposed method will be also higher.

5. CONCLUSIONS AND FUTURE WORK

In this paper, a new image steganography enhancement method has been presented for hiding data in the images. This enhancement method is used in MHC and PSNR of PVD method by using Mobile MPK Coding and it has been called (PVD-MPK). The enhancement method is combined with the MSLDIP-MPK method to increase the capacity. By using our enhancement method, the MHC of the cover image and the PSNR of stego image have been improved. In the smooth areas, the secret data has been hidden into the cover image using our enhancement PVD-MPK method for achieving better quality. While, the MSLDIP-MPK method is used in the edge areas for achieving more capacity. Experimental results showed that our proposed enhancement method can be used to hide much more information than that other existed methods and the visual quality of the stego image is also improved.

In the future work, we are looking forward to try applying the proposed method on audio and video and check the validity of our method on other carriers not only images. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher.

6. REFERENCES

[1] K. R. Babu et al, "A Survey on Cryptography and Steganography Methods for Information Security," International Journal of Computer Applications (0975 – 8887), Vol. 12, No.2, PP. 13-17, November 2010

[2] K. Nitin K and N. Ashish V, "Comparison of Various Images Steganography Techniques," International Journal of Computer Science and Management Research, Vol 2, Issue 1, PP. 1213 – 1217, January 2013.

[3] S. Sharda and S. Budhiraja, "Image Steganography: A Review," International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.4, Issue 1, PP. 707–710, January 2013.

[4] C.-K. Chan, and L.M. Cheng, "Hiding data in image by simple LSB substitution," Pattern Recognition, Vol. 37, Issue 3, PP. 469 – 474, 2004.

[5] A. J. Raphael, and V. Sundaram, "Cryptography and Steganography – A Survey," International Journal, ISSN: 2229-6093, Vol 2 (3), PP. 626- 630, 2011.

[6] A. A . Radwan, A. Swilem, and A.-H. Seddik, "A High Capacity SLDIP (Substitute Last Digit in Pixel) Method," Fifth international conference on intelligent computing and information systems (ICICIS 2011), Ain Shams University, Egypt, 30 June – 3 July, PP. 156- 160, 2011.

[7] A. A. J. Altaay et al, "An Introduction to Image Steganography Techniques," International Conference on Advanced Computer Science Applications and Technologies, PP. 122 - 126, 2012.

[8] S. Thanekar, S. S. Pawar , " OCTA (STAR) PVD: A Different Approach of Image Steganopgraphy," IEEE International Conference on Computational Intelligence and Computing Research, PP. 1 – 5, 2013.

[9] 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," IEE Proceedings - Vision, Image and Signal Processing, Volume 152, Issue 5, PP. 611 – 615, October 2005,

[10] C.-M. Wang, N.-I. Wu, C.-S. Tsai, "A High Quality Steganographic Method with Pixel Value Differencing and Modulus Function," Journal of Systems and Software, Vol. 81, Issue 1, PP. 150-158, 2008.

[11] C.H. Yang, C.Y. Weng, S.J. Wang, 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, PP. 488 – 497, September 2008.

[12] K. C. Chang, C. P. Chang, P. S. Huang and T. m. Tu, "A Novel Image Steganographic Method Using Tri-Way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No. 2, PP. 37 - 44, June 2008.

[13] H.B. Kekre, P. Halarnkar, and K. Dhamejani, "Capacity Increase for Information Hiding Using Maximum Edged Pixel Value Differencing," Springer-Verlag Berlin Heidelberg , PP. 190–194, 2011.

[14] M. Sabokdast and M. Mohammadi, "A Steganographic Method for Images with Modulus Function and Modified LSB Replacement Based on PVD," 5th Conference on Information and Knowledge Technology (IKT), PP. 121 - 126, May 2013.

[15] A. A. Ali and A.-H. S. Saad , “New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding),” International Journal of Computer Applications, Vol. 59, No.15, PP. 0975 – 8887, December 2012.

[16] D.-C. Wu, and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognition Letters, Vol. 24, PP. 1613–1626, 2003.

[17] J.-C. Joo, H.-Y. Lee, and H.-K. Lee, “Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function”, EURASIP Journal on Advances in Signal Processing, PP.1–13, 2010