Pertanika J. Sci. & Technol. 27 (2): 753 - 768 (2019)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

A Novel Multi Stego-image based Data Hiding Method for Gray Scale Image

Aditya Kumar Sahu[1]* and Gandharba Swain[2]

[1,2]Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[1]Department of Computer Science and Engineering, GMRIT, Rajam, Andhra Pradesh, India

ABSTRACT

In this paper, we present a novel multi stego-image based data hiding method using the principle of the modified least significant bit (LSB) matching to improve the embedding capacity (EC) as well as image quality. Initially, each original pixel produces four new pixels. The secret data is hidden in all the four produced pixels. Then the pixels are readjusted to improve the quality of the stego-images. There are four separate stego-images developed from the four different readjusted pixels. Each stego-image hides one bit per pixel. The average peak signal-to-noise ratios (PSNR) for the stego-images are 36.06 dB, 37.88 dB, 39.60 dB and 41.00 dB respectively. Furthermore, the proposed method successfully withstand against RS-steganalysis.

Keywords: Data hiding, LSB Matching, RS-analysis, steganography

ARTICLE INFO

Article history:
Received: 4 May 2018
Accepted:12 September 2018
Published: 25 April 2019

E-mail addresses:
adityasahu.cse@gmail.com (Aditya Kumar Sahu)
gswain1234@gmail.com (Gandharba Swain)
* Corresponding author

INTRODUCTION

Over the years, steganography has emerged as an elementary and conducive choice to transmit digital data (Cheddad et al., 2010). Steganography is the art of covert communication (Johnson & Jajodia, 1998). Here the data transmission accomplishes through various cover mediums such as image, audio, video, and text. Image steganography use image to carry the information through the public channel

ISSN: 0128-7680
e-ISSN: 2231-8526

(Subhedar & Mankar, 2014). It is a convenient approach in the fields of defense, healthcare, and banking sector where secrecy is the top priority (Cheddad et al., 2010). Image steganography is achieved in 2 ways (1) reversible (2) irreversible (Subhedar & Mankar, 2014). The reversible approach ensures the retrieval of secret data as well as the original image at the receiver side. Whereas the irreversible approaches focus only on the successful retrieval of secret data. Our proposed work is based on the irreversible approach. Irreversible methods such as LSB, LSB matching, pixel value differencing (PVD), exploiting modification direction (EMD) and modulus function (MF) are some of the prominent methods in the field of image steganography (Hussain et al., 2018).

The image quality and EC are the two image steganographic parameters to gauge the efficacy of a data hiding method. The image quality depends on the distortion of the stego-image. Various image quality assessment (IQA) metrics such as; (i) mean square error (MSE), (ii) peak signal-to-noise ratio (PSNR), (iii) root mean square error (RMSE), (iv) Weighted PSNR (WPSNR) (v) The universal image quality index (Q), and (vi) structural similarity (SSIM) index exists in literature (Pradhan et al., 2016). PSNR measures the visual quality (Bong & Khoo, 2015) of a stego-image. The high PSNR is an indication of lower distortion and vice versa. The MSE compares the original and stego-image to measure the quality of stego-image. It should be as low as possible (Bong & Khoo, 2014). Further, the WPSNR uses MSE and Noise Visibility Function (NVF) to gauge the quality of the stego-image. Similarly, Q and SSIM are also used to measure the stego-image quality (Wang, et al., 2004). The Q should always be at upper side i.e. approximately 1for the better quality of stego-image. The EC is the number of secret data bits the image can conceal without noticeable artifacts (Hussain et al., 2018).

The simplicity and straightforwardness of the least significant bit (LSB) image steganography methods made it convenient for information hiding. Johnson and Jajodia (1998) concealed the secret data by replacing the LSB of the original image pixel. This method was susceptible to the intruder as by accessing the LSBs, the data can be easily accessed. In recent years, voluminous articles have been proposed using LSB methods (Wu & Hwang, 2017; Wang et al., 2001; Chan & Cheng, 2004; Yang et al., 2009; Sahu & Swain, 2016, Sahu & Swain, 2017, Sahu & Swain, 2018, Sahu et al., 2018). Sharp (2001) proposed the LSB matching to lower the distortion of the stego-image by randomly performing +1 or -1 to the original pixel values in case if the secret data did not match with the LSB. This method limits the embedding capacity to one bit per pixel. Mielikainen (2006) came with an alteration to the LSB method called LSB matching revisited. Here the secret bits are concealed with the help of the binary function and four embedding rules. The suggested method also produces the same embedding capacity as produced by Sharp (2001) but it modifies fewer bits in the original image.

Though LSB approaches greatly enhance the embedding capacity, it is exposed to RS-analysis (Fridrich & Goljan, 2002). With the motive to increase the capacity and lowering the distortion to the stego-image, Wu and Tsai (2003) proposed pixel values differencing (PVD) method. The pixels are bifurcated into blocks with 2 pixels each and then the difference value (d) between the two pixels is computed. The value d is mapped to the specified range table in order to identify the number secret data bits to be embedded inside a block. Wang et al. (2008) found the solution for the falling-off boundary problem (FOBP) which existed in Wu and Tsai (2003) by bringing together the PVD and modulus function. Wang et al. (2008) method enhanced the PSNR value as compared to Wu and Tsai (2003). To expel the restriction of capacity in original PVD, Chang et al. (2008) introduced Tri-way pixel value differencing (TPVD) method. It finds the difference value d in three directions such as horizontal, vertical and diagonal by choosing a reference point. Swain (2016) proposed contemporary adaptive directional PVD method which contributed by significant upgradation in the embedding capacity as well as retaining the image quality. There are large number of articles in literature utilizing the advantage of PVD methods (Shen et al., 2015; Lee et al., 2012; Hameed et al., 2017; Lu et al., 2006; Hussain et al., 2017).

LSB substitution methods offer larger capacity whereas PVD methods attain better imperceptibility. Methods such as LSB and PVD when combined they outperform others in terms of capacity and imperceptibility (Khodaei & Faez, 2012; Hussain et al., 2016; Wu et al., 2005; Jung, 2018; Swain, 2018).

The existing image steganographic methods produce single stego-image from the original image. The restriction of single stego-image limits the EC. Various methods in literature made an attempt to increase the EC, but at the same time, the image quality reduced (Jung, 2018; Khodaei & Faez, 2012). In this paper, we present a novel multi stego-image based method to conceal the secret data. The proposed method produces four stego images from one original image. Each pixel of the produced stego-images hides one bit.

RELATED WORK

Wu and Hwang's (2017) Method

Wu and Hwang (2017) proposed a novel LSB substitution method to reduce the distortion to of the stego-image. It conceals 3 bits in a group of 3 pixels with maximum modification of +1 or -1 to each pixel. The expected number of modifications per pixel (ENMPP) is reduced compared to the conventional LSB substitution methods. The reduction in the ENMPP results in an enhanced image quality. However, the capacity remains the same i.e. 1 bit per pixel. The step by step explanation of Wu and Hwang's (2017) method is explained in this section, followed by an example shown in Figure 1.

Step 1: At first take 3 pixels P_1, P_2 and P_3 from the original image horizontally.
Step 2: Now, represent P_1, P_2 and P_3 to its corresponding binary such as $P_1 = a_1a_2a_3a_4a_5a_6a_7a_8$, $P_2 = b_1b_2b_3b_4b_5b_6b_7b_8$ and $P_3 = c_1c_2c_3c_4c_5c_6c_7c_8$.

Now, compute X, Y, Z values using equation (1-3).

$$X = a_8 \oplus a_7 \oplus b_8 \tag{1}$$

$$Y = b_8 \oplus b_7 \oplus c_8 \tag{2}$$

$$Z = c_8 \oplus c_7 \oplus a_8 \tag{3}$$

Step 3: Let, s_1, s_2 and s_3 be the 3 secret bits.
Step 4: Now, update the value of, P_1, P_2 and P_3 using the given condition below. Here $==$ is the bit comparison operator and && is logical AND operator.

if $(X == s_1)$ && $(Y == s_2)$ && $(Z == s_3)$
    then, $P_1 = P_1$, $P_2 = P_2$ and $P_3 = P_3$
else if $(X \neq s_1)$ && $(Y == s_2)$ && $(Z == s_3)$
    if $P_2 \bmod 2 = 0$, then $P_2 = P_2 - 1$.
    else $P_2 = P_2 + 1$.
    end
else if $(X == s_1)$ && $(Y \neq s_2)$ && $(Z == s_3)$
    if $P_3 \bmod 2 = 0$, then $P_3 = P_3 - 1$.
    else $P_3 = P_3 + 1$.
    end
else if $(X == s_1)$ && $(Y == s_2)$ && $(Z \neq s_3)$
    if $P_1 \bmod 2 = 0$, then $P_1 = P_1 - 1$.
    else $P_1 = P_1 + 1$.
    end
else if $(X \neq s_1)$ && $(Y \neq s_2)$ && $(Z == s_3)$
    if $P_2 \bmod 2 = 0$, then $P_2 = P_2 + 1$.
    else $P_2 = P_2 - 1$.
    end
else if $(X == s_1)$ && $(Y \neq s_2)$ && $(Z \neq s_3)$
    if $P_3 \bmod 2 = 0$, then $P_3 = P_3 + 1$.
    else $P_3 = P_3 - 1$.
    end

else if $(X \neq s_1)$ && $(Y == s_2)$ && $(Z \neq s_3)$

  if $P_1 \bmod 2 = 0$, then $P_1 = P_1 + 1$.

  else $P_1 = P_1 - 1$.

  end

else if $(X \neq s_1)$ && $(Y \neq s_2)$ && $(Z \neq s_3)$

  if $P_3 \bmod 2 = 0$, then $P_3 = P_3 - 1$.

  else $P_3 = P_3 + 1$.

  end

  if $P_1 \bmod 2 = 0$, then $P_1 = P_1 + 1$.

  else $P_1 = P_1 - 1$.

  end

end

Step 2: Obtain the stego-pixels as $P_1^* = P_1$, P_2^*, P_2 and $P_3^* = P_3$

Step 3: At the receiver side, retrieve the stego-pixels as P_1^* , P_2^* and P_3^*. Now find the secret data s_1, s_2 and s_3 from the stego-pixels using the same equations (1), (2) and (3), assuming $s_1 = X$, $s_2 = Y$ and $s_3 = Z$. Figure 1 shows the embedding and extraction example for Wu and Hwang's (2017) method.

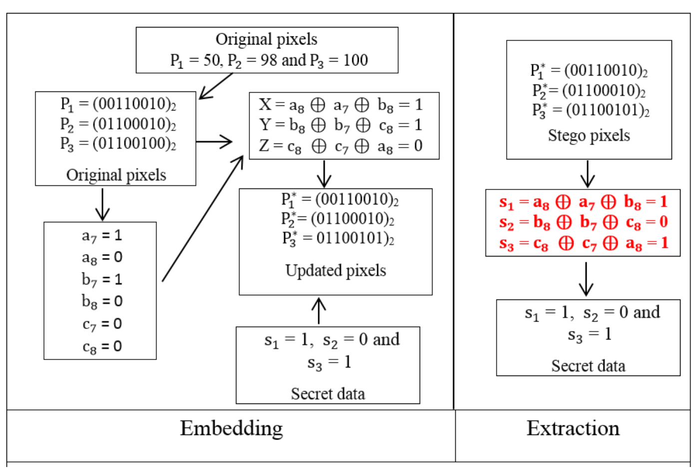


Figure 1. Example for Wu and Hwang's (2017) method

PROPOSED METHOD

The step by step embedding and extraction procedure for the proposed method is presented in this section. The pixels of an image are processed in raster scan order to conceal the secret data. Let P_i be the ith pixel.

Embedding Steps

Step 1: Obtain P_{i1}, P_{i2}, P_{i3} and P_{i4} from P_i using equation (4)

$$P_{i1} = \left\lfloor \frac{P_i}{4} \right\rfloor, P_{i2} = \left\lfloor \frac{P_i}{4} \right\rfloor, P_{i3} = \left\lfloor \frac{P_i}{4} \right\rfloor \text{ and } P_{i4} = \left\lfloor \frac{P_i}{4} \right\rfloor \qquad [4]$$

Step 2: Find the remainder (rmd) using equation (5) and update P_{i1}, P_{i2}, P_{i3} and P_{i4} using equation (6-9).

$$rmd = P_i \bmod 4 \qquad [5]$$

$$P_{i1} = \begin{cases} P_{i1} + 1, \text{if rmd } = 3 \text{ or } 2 \text{ or } 1 \\ P_{i1,} \text{ if rmd } = 0 \end{cases} \qquad [6]$$

$$P_{i2} = \begin{cases} P_{i2} + 1, \text{if rmd } = 3 \text{ or } 2 \\ P_{i2,} \text{ if rmd } = 0 \text{ or } 1 \end{cases} \qquad [7]$$

$$P_{i3} = \begin{cases} P_{i3} + 1, \text{if rmd } = 3 \\ P_{i3,} \text{ if rmd } = 0 \text{ or } 1 \text{ or } 2 \end{cases} \qquad [8]$$

$$P_{i4} = \{P_{i4,} \text{ if rmd } = 0 \text{ or } 1 \text{ or } 2 \text{ or } 3 \qquad [9]$$

Step 3: Let s_1, s_2, s_3 and s_4 be the secret data in binary.

Step 4: Obtain the binary values of P_{i1}, P_{i2}, P_{i3} and P_{i4} and store in bin_1, bin_2, bin_3 and bin_4 respectively.

Step 5: if $LSB(bin_1) == s_1$

then, $P_{i1} = P_{i1}$

else $P_{i1} = P_{i1} + 1$

Step 6: Find sum_1 using equation (10).

$$sum_1 = \left\lfloor \frac{P_{i1}}{2} \right\rfloor + P_{i2} \qquad [10]$$

Let bin_{sum1} is the corresponding binary of sum_1.

Step 7: if $LSB(bin_{sum1}) == s_2$

then $P_{i2} = P_{i2}$

else $P_{i2} = P_{i2} + 1$

Step 8: if $LSB(bin_3) == s_3$

then $P_{i3} = P_{i3}$

else $P_{i3} = P_{i3} + 1$

Step 9: Find sum_2 using equation (11).

$$sum_2 = \left\lfloor \frac{P_{i3}}{2} \right\rfloor + P_{i4} \qquad [11]$$

Let bin_{sum2} is the corresponding binary of sum_2.

If $LSB(bin_{sum2}) == s_4$

then $P_{i4} = P_{i4}$

else $P_{i4} = P_{i4} + 1$

Step 10: Obtain the four stego pixels for the pixels P_{i1}, P_{i2}, P_{i3} and P_{i4} using equation (12)

$$P_{i1}^{*} = P_{i1} \times 4$$
$$P_{i2}^{*} = P_{i2} \times 4 \quad [12]$$
$$P_{i3}^{*} = P_{i3} \times 4$$
$$P_{i4}^{*} = P_{i4} \times 4$$

Step 11: Create four stego-images using P_{i1}^{*}, P_{i2}^{*}, P_{i3}^{*} and P_{i4}^{*}.

Step 12: The embedding is done.

Extraction Steps

Step 1: Suppose the ith stego-pixels of the 4 stego-images are P_{i1}^{*}, P_{i2}^{*}, P_{i3}^{*} and P_{i4}^{*}. Compute P_{i1}^{**}, P_{i2}^{**}, P_{i3}^{**} and P_{i4}^{**} using equation (13)

$$P_{i1}^{**} = \frac{P_{i1}^{*}}{4}$$
$$P_{i2}^{**} = \frac{P_{i2}^{*}}{4} \quad [13]$$
$$P_{i3}^{**} = \frac{P_{i3}^{*}}{4}$$
$$P_{i4}^{**} = \frac{P_{i4}^{*}}{4}$$

Step 2: Let bin_1^{*} and bin_3^{*} be the eight bit binary for P_{i1}^{**} and P_{i3}^{**}.

Step 3: Compute sum_{s1} using equation (14)

$$sum_{s1} = \left\lfloor \frac{P_{i1}^{**}}{2} \right\rfloor + P_{i2}^{**} \quad [14]$$

Represent sum_{s1} to its eight binary bits and store in bin_2^{*}.

Step 4: Compute sum_{s2} using equation (15)

$$sum_{s2} = \left\lfloor \frac{P_{i3}^{**}}{2} \right\rfloor + P_{i4}^{**}. \quad [15]$$

Represent sum_{s2} to its eight binary bits and store in bin_4^{*}.

Step 5: Obtain s_1, s_2, s_3, s_4 using equation (16)

$$s_1 = LSB(bin_1^{*})$$
$$s_2 = LSB(bin_2^{*}) \quad [16]$$
$$s_3 = LSB(bin_3^{*})$$
$$s_4 = LSB(bin_4^{*})$$

Step 6: s_1, s_2, s_3, s_4 are the 4 extracted bits.

Step 7: The extraction is done.

EXAMPLE FOR THE PROPOSED METHOD

Embedding Steps

Step 1: Let the original pixel be $P_i = 123$ and the secret bits in binary are 0010.

Step 2: Now find $P_{i1} = 30$, $P_{i2} = 30$, $P_{i3} = 30$ $P_{i4} = 30$ using equation (4).

Step 3: Obtain the remainder, rmd = 3 using equation (5) and compute $P_{i1} = 31$, $P_{i2} = 31$, $P_{i3} = 31$ and $P_{i4} = 30$ using equations (6), (7), (8) and (9) respectively.

Step 4: Now obtain the corresponding eight bit binary for P_{i1}, P_{i2}, P_{i3} and P_{i4} as $bin_1 = 00011111$, $bin_2 = 00011111$, $bin_3 = 00011111$ and $bin_4 = 00011110$.

Step 5: As $LSB(bin_1) \neq 0$, so $P_{i1} = 32$.

Step 6: Obtain $sum_1 = \left\lfloor \frac{P_{i1}}{2} \right\rfloor + P_{i2} = 47$ using equation (10) and $bin_{sum1} = 00101111_2$.

Step 7: As $LSB(bin_{sum1}) \neq 0$, so, $P_{i2} = P_{i2} + 1 = 32$

Step 8: Again $LSB(bin_3) = 1$, so, $P_{i3} = 31$.

Step 9: Now $sum_2 = \left\lfloor \frac{P_{i3}}{2} \right\rfloor + P_{i4} = 45$ equation (11) and $LSB(bin_{sum2}) \neq 0$, hence $P_{i4} = 31$.

Step 10: The final stego-pixels are $P_{i1}^* = 128$, $P_{i2}^* = 128$, $P_{i3}^* = 124$ and $P_{i4}^* = 124$ computed using equation (12)

Step 11: The embedding is done.

Extraction Steps

Step 1: The four stego-pixels are $P_{i1}^* = 128$, $P_{i2}^* = 128$, $P_{i3}^* = 124$ and $P_{i4}^* = 124$.

Step 2: Obtain the values of $P_{i1}^{**} = 32$, $P_{i2}^{**} = 32$, $P_{i3}^{**} = 31$ and $P_{i4}^{**} = 31$ using equation (13).

Step 3: Obtain $bin_1^* = 00100000$ and $bin_3^* = 00011111$.

Step 4: Compute $sum_{s1} = 48$ using equation (14). So, $bin_2^* = 00110000$.

Step 5: Compute $sum_{s2} = 46$ using equation (15). So, $bin_4^* = 00101110$.

Step 6: Obtain s_1, s_2, s_3, s_4 using equation (16) as $s_1 = 0$, $s_2 = 0$, $s_3 = 1$ and $s_4 = 0$.

Step 7: The extraction is done.

RESULTS AND DISCUSSION

The experiment had been conducted using Matlab tool. The images were taken from USC–SIPI and CV online databases and three of them are shown in Figure 2. The proposed method had been compared with existing methods (Wu & Hwang, 2017, Wu & Tsai, 2003, Khodaei & Faez, 2012 and Jung, 2018) and 1-LSB, 2-LSB and 3-LSB substitution with respect to the image steganographic parameters such as embedding capacity and PSNR. The PSNR can be computed using equation (17).

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\mathrm{MSE}} \quad [17]$$

Where MSE is the mean square error and can be found using equation (18).

$$\mathrm{MSE} = \frac{1}{m \times n} \Sigma_{i=1}^{m} \Sigma_{j=1}^{n} \left(x_{ij} - y_{ij}\right)^{2} \quad [18]$$

Where, x_{ij} and y_{ij} are the pixel values for the original and stego-image at position (i, j) respectively.

(a) (b) (c)

Figure 2. Original images (a) Lighthouse, (b) Boat and (c) Zelda

The proposed method produces four different stego-images from one original image. The modified LSB matching method hides one bit per each produced stego-image. So, for four stego-images the total bits hidden are four times of 262144 bits. Again, due to hiding one bit per pixel, the distortion caused to the image is significantly reduced. The results of PSNR and EC for the proposed method and the other existing methods are presented in Tables 1, 2, 3, 4, 5 and 6. The average PSNR for the stego-images 1 to 4 are 36.06 dB, 37.88 dB, 39.60 dB and 41.00 dB respectively. The PSNR for Wu and Hwang (2017) is 51.69 dB but its capacity is limited to 262144 bits only. The embedding capacity of Jung (2018) is 916317 bits with a significant reduction in image quality i.e. with PSNR of 31.17 dB only. Further, the PSNR for Wu & Tsai, (2003) and Khodaei & Faez (2012) are 40.27 dB, 37.45 dB with EC having 407125 and 794816 bits respectively. Hence from the above analysis, we conclude that the proposed method is superior in terms of embedding capacity and PSNR.

Table 1

PSNR for the proposed method

Peak signal-to-noise ratio (PSNR)				
Images 512×512	Stego-image1	Stego-image 2	Stego-image 3	Stego-image 4
Lighthouse	36.00	37.64	39.52	40.96
Boat	36.01	37.85	39.46	40.86
Zelda	36.32	38.12	39.99	41.31
Crowd	35.86	37.83	39.71	40.99
Girlface	36.32	38.12	39.99	41.31
Clown	36.19	38.34	39.12	40.81
Trucks	36.02	37.63	39.39	40.98
Kiel	35.92	37.73	39.57	40.94
Aerial	35.92	37.73	39.59	40.91
Airfield	36.08	37.82	39.75	41.00
Average	**36.06**	**37.88**	**39.60**	41.00

Table 2

PSNR for 1-LSB, 2-LSB, 3-LSB

Peak signal-to-noise ratio (PSNR)			
Images 512×512	1-LSB	2-LSB	3-LSB
Lighthouse	51.63	44.63	38.44
Boat	51.61	44.55	38.47
Zelda	51.63	44.65	38.47
Crowd	51.63	44.66	38.46
Girlface	51.66	44.65	38.45
Clown	51.63	44.64	38.46
Trucks	51.63	44.64	38.45
Kiel	51.66	44.65	38.45
Aerial	51.68	44.62	38.46
Airfield	51.69	44.64	38.47
Average	**51.64**	**44.63**	**38.45**

Table 3
PSNR Wu & Hwang, 2017b, Wu & Tsai, 2003a, Khodaei & Faez, 2012 and Jung, 2018

Peak signal-to-noise ratio (PSNR)				
Images 512×512	Wu & Hwang, 2017b	Wu & Tsai, 2003a	Khodaei & Faez, 2012	Jung, 2018
Lighthouse	51.79	40.13	36.56	31.20
Boat	52.01	38.98	34.72	31.21
Zelda	51.92	41.13	38.28	31.01
Crowd	51.23	39.56	38.87	31.22
Girlface	51.45	41.41	37.14	31.11
Clown	51.96	39.51	38.54	31.19
Trucks	51.90	41.01	37.72	31.23
Kiel	51.47	40.45	38.34	31.04
Aerial	51.56	40.99	37.01	31.01
Airfield	51.65	39.53	37.34	31.49
Average	**51.69**	**40.27**	**37.45**	**31.17**

Table 4
EC for the proposed method

Embedding capacity (EC)				
Images 512×512	Stego-image 1	Stego-image 2	Stego-image 3	Stego-image 4
Lighthouse	262144	262144	262144	262144
Boat	262144	262144	262144	262144
Zelda	262144	262144	262144	262144
Crowd	262144	262144	262144	262144
Girlface	262144	262144	262144	262144
Clown	262144	262144	262144	262144
Trucks	262144	262144	262144	262144
Kiel	262144	262144	262144	262144
Aerial	262144	262144	262144	262144
Airfield	262144	262144	262144	262144
Average	**262144**	**262144**	**262144**	262144

Table 5

EC for 1-LSB, 2-LSB and 3-LSB

Images 512×512	1-LSB	2-LSB	3-LSB
Lighthouse	262144	524288	786432
Boat	262144	524288	786432
Zelda	262144	524288	786432
Crowd	262144	524288	786432
Girlface	262144	524288	786432
Clown	262144	524288	786432
Trucks	262144	524288	786432
Kiel	262144	524288	786432
Aerial	262144	524288	786432
Airfield	262144	524288	786432
Average	**262144**	**524288**	**786432**

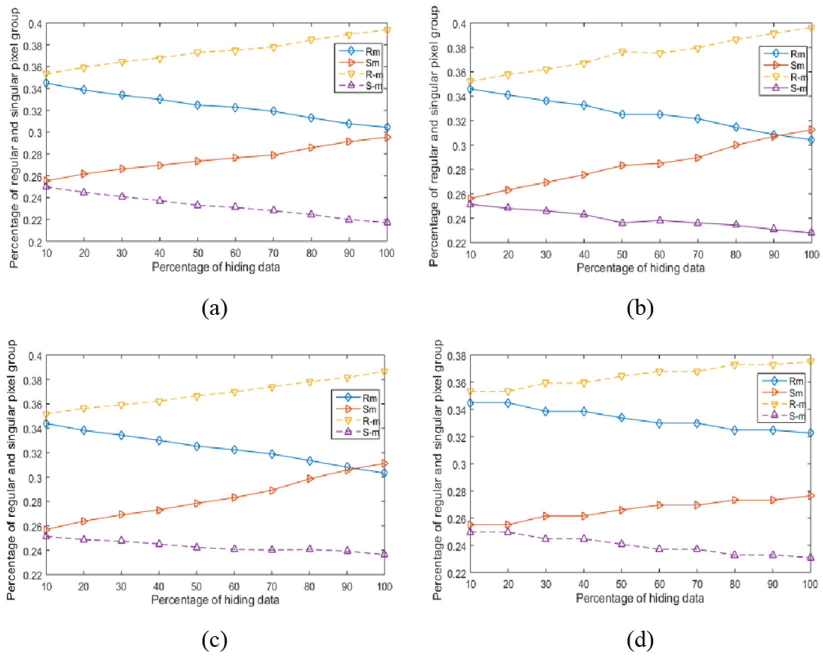
Table 6

EC for Wu & Hwang, 2017b, Wu & Tsai, 2003a, Khodaei & Faez, 2012 and Jung, 2018

Images 512×512	Wu & Hwang, 2017b	Wu & Tsai, 2003a	Khodaei & Faez, 2012	Jung, 2018
Lighthouse	262144	410395	797234	919301
Boat	262144	420267	790398	919103
Zelda	262144	398890	791608	915980
Crowd	262144	421413	799168	919003
Girlface	262144	386769	790039	915474
Clown	262144	421491	797702	915127
Trucks	262144	398324	794670	914501
Kiel	262144	399813	794891	917801
Aerial	262144	391910	795560	914571
Airfield	262144	421980	796890	912307
Average	**262144**	**407125**	**794816**	**916317**

RS-analysis

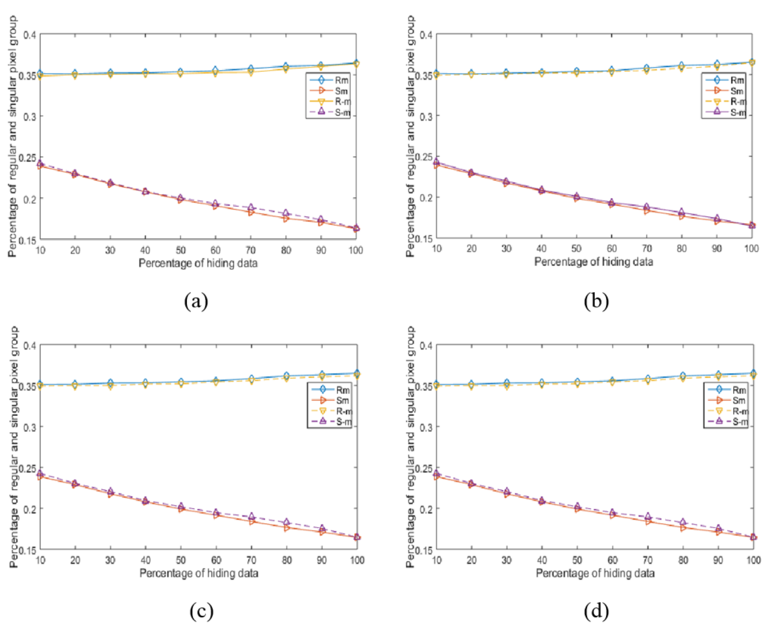
The RS-analysis is based on the dual statistical method. The pixels are categorized into 3 groups such as (1) the regular group with R_M and R_{-M}, (2) the singular group with S_M and, S_{-M} and (3) the unusable group. The discrimination function (DF) finds the value of R_M and R_{-M}, S_M and S_{-M}.



(a) (b)

(c) (d)

Figure 3. RS-plot for (a) 1-LSB, (b) 2-LSB, (c) 3-LSB and (d) Jung (2018)



(a) (b)

(c) (d)

Figure 4. RS-plot for the proposed method (a) stego-image 1, (b) stego-image 2, (c) stego-image 3 and (d) stego-image 4

In the resulting RS-plot, the x-axis represents the percentage of hiding capacity and the y-axis represents the percentage of regular or singular groups at the various level of embedding. From the obtained plot If the condition, $R_M \approx R_{-M} > S_M \approx S_{-M}$ holds then it implies that the said technique has successfully passed the RS-analysis. Otherwise, if the condition $R_{-M} - S_{-M} > R_M - S_M$ holds then the technique is exposed to RS-analysis. The RS-plots for the 1-LSB, 2-LSB, 3-LSB substitutions and Jung's (2018) method are shown in Figure 3, it is clearly observed that the condition $R_{-M} - S_{-M} > R_M - S_M$ is satisfying and hence these methods are caught by RS-analysis. Whereas RS-plots for the proposed method for the boat image with four stego-images are shown in Figure 4, it can be observed the condition $R_M \approx R_{-M} > S_M \approx S_{-M}$ holds for the proposed method. Hence from the above analysis it is found that the proposed method is resistant to RS-analysis.

CONCLUSION AND FUTURE SCOPE

This paper proposes a novel way of data hiding using multi stego-images to achieve high capacity with low distortion. First, each pixel of the original image produces four pixels. The secret data is hidden on each of the produced pixels using the modified LSB matching method. Then pixels are readjusted to reduce the distortion. In this way, the original image produces four different stego-images and each stego-image hides 1 bit per pixel. Further, the proposed method resists RS-analysis. For further improvement, the authors aim to develop a reversible steganography by improving the EC for the individual stego-images by combining LSB matching with PVD.

ACKNOWLEDGMENTS

We are thankful to the editor and the anonymous reviewers for their suggestions and comments. We declare this work is an independent work and no financial assistance has been received for this work.

REFERENCES

Bong, D. B. L., & Khoo, B. E. (2014). Blind image blur assessment by using valid reblur range and histogram shape difference. *Signal Processing: Image Communication, 29*(6), 699-710.

Bong, D. B. L., & Khoo, B. E. (2015). Objective blur assessment based on contraction errors of local contrast maps. *Multimedia Tools and Applications*, *74*(17), 7355-7378.

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern recognition, 37*(3), 469-474

Chang, K. C., Chang, C. P., Huang, P. S., & Tu, T. M. (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing. *Journal of Multimedia, 3*(2), 37-44.

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727-752.

Fridrich, J., & Goljan, M. (2002, April 29). Practical steganalysis of digital images: state of the art. In *Security and Watermarking of Multimedia Contents IV* (Vol. 4675, pp. 1-14). San Jose, California, United States.

Hameed, M. A., Aly, S., & Hassaballah, M. (2017). An efficient data hiding method based on adaptive directional pixel value differencing (ADPVD). *Multimedia Tools and Applications, 77*, 14705-14723.

Hussain, M., Wahab, A. W. A., Javed, N., & Jung, K. H. (2016). Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. *Symmetry, 8*(6), 41-61.

Hussain, M., Wahab, A. W. A., Ho, A. T., Javed, N., & Jung, K. H. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. *Signal Processing: Image Communication, 50*, 44-57.

Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication, 65*, 46-66.

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26-34

Jung, K. H. (2018). Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. *Journal of Real-Time Image Processing, 14*(1), 127-136.

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.

Lee, Y. P., Lee, J. C., Chen, W. K., Chang, K. C., Su, J., & Chang, C. P. (2012). High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information Sciences, 191*, 214-225.

Lu, H. C., Chu, Y. P., & Hwang, M. S. (2006). New steganographic method of pixel value differencing. *Journal of Imaging Science and Technology, 50*(5), 424-426.

Mielikainen, J. (2006). LSB matching revisited. *IEEE Signal Processing Letters, 13*(5), 285-287.

Pradhan, A., Sahu, A. K., Swain, G., & Sekhar, K. R. (2016, May 6-7). Performance evaluation parameters of image steganography techniques. In *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)* (pp. 1-8). Bangalore, India.

Sahu, A. K., & Swain, G. (2016). A Review on LSB substitution and PVD based image steganography techniques. *Indonesian Journal of Electrical Engineering and Computer Science, 2*(3), 712-719.

Sahu, A. K., & Swain, G. (2017). Information Hiding Using Group of Bits Substitution”. *International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), 7*(2), 162-167.

Sahu, A. K., & Swain, G. (2018). An Improved Data Hiding Technique Using Bit Differencing and LSB Matching. *Internetworking Indonesia, 10*(1), 17-21.

Sahu, A. K., Swain, G., & Babu, E. S. (2018). Digital Image Steganography Using Bit Flipping. *Cybernetics and Information Technologies, 18*(1), 69-80.

Sharp, T. (2001, April 25-27). An implementation of key-based digital signal steganography. In *International Workshop on Information Hiding* (pp. 13-26). Pittsburgh, PA, USA.

Shen, S., Huang, L., & Tian, Q. (2015). A novel data hiding for color images based on pixel value difference and modulus function. *Multimedia Tools and Applications*, *74*(3), 707-728.

Subhedar, M. S., & Mankar, V. H. (2014). Current status and key issues in image steganography: A survey. *Computer Science Review*, *13*, 95-113.

Swain, G. (2016). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimedia Tools and Applications*, *75*(21), 13541-13556.

Swain, G. (2018). Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. *Arabian Journal for Science and Engineering, 2018*, 1-10. doi: https://doi.org/10.1007/s13369-018-3372-2.

Wang, R. Z., Lin, C. F., & Lin, J. C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. *Pattern Recognition*, *34*(3), 671-683.

Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, *81*(1), 150-158.

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE Transactions on Image Processing*, *13*(4), 600-612.

Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*(9-10), 1613-1626.

Wu, N. I., & Hwang, M. S. (2017). A novel LSB data hiding scheme with the lowest distortion. *The Imaging Science Journal*, *65*(6), 371-378.

Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings-Vision, Image and Signal Processing*, *152*(5), 611-615.

Yang, H., Sun, X., & Sun, G. (2009). A high-capacity image data hiding scheme using adaptive LSB substitution. *Radioengineering*, *18*(4), 509-516.