Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion

Biswapati Jana[1], Debasis Giri[2] and Shyamal Kumar Mondal[3]
(Corresponding author: Biswapati Jana)
Department of Computer Science, Vidyasagar University[1]
Midnapore, Pin-721102, India
(Email: biswapatijana@gmail.com)
Department of Computer Science and Engineering, Haldia Institute of Technology[2]
Department of Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University[3]
(Received June 22, 2015; revised and accepted Aug. 12 & Aug. 22, 2015)

Abstract

In this paper, we propose a dual-image based reversible data hiding scheme. Here, we divide a secret message into sub-stream of size n bits, where $n-1$ bits are embedded using Pixel Value Differencing (PVD) and 1 bit is embedded using Difference Expansion (DE). We consider two consecutive pixels from cover image, calculate the difference between them and then embed $n-1$ bits secret message by modifying the pixel pair. Again, we consider that modified pixel pair to embed 1 bit secret message using embedding function. After that, we distribute these two stego pixel pairs among dual image depending on a shared secret key bit stream. At the receiver end, we extract the secret message successfully and recover original cover image from dual stego image without any distortion. Finally, we compare our scheme with other state-of-the-art methods and obtain reasonably better performance in terms of data embedding capacity.

Keywords: Difference expansion, dual image, pixel value differencing, reversible data hiding

1 Introduction

Steganography is one of the most commonly used protective method for information security. Steganography can be classified into two categories: irreversible and reversible. In irreversible technique, the secret data can be embedded and extracted successfully, but the original image might not be recovered [1, 5, 6, 8, 23]. On the other hand, reversible data hiding schemes [9, 10, 16, 17, 19, 20, 22, 24] are capable of embedding the secret message as well as can extract the secret message and recover the original image. Two important measures of reversible data hiding are embedding capacity and distortion of cover work. In recent years, a bunch of research [7, 13, 14, 15, 21, 27] have been performed to improve the embedding capacity and to minimize the distortion which is the objective of data hiding schemes. Wu and Tsai [26] proposed a data embedding method based on PVD, where, the difference of two adjacent pixels in the cover image is calculated. The number of bits to be embedded into these two pixels are determined by their absolute difference and a pre-defined reference table. By modifying these two pixel values, data bits can be embedded. Because the same range in the reference table will be referred before and after data embedding, the same number of secret data bits can be determined and thus the embedded secret data bits can be exactly extracted. Tian [22] proposed a difference expansion data hiding approach to conceal the secret data into the difference of a pair consecutive pixel values with high payload size. Lee et al. [13] utilized the histogram of the difference of pixel values to embed the secret data in host image for improving the quality of marked-images. Ni et al. [16] proposed reversible data hiding technique which is based on histogram shifting with zero or minimum change of the pixel gray values. Being reversible, both the original and the embedded data can be completely restored. Thodi et al. [21] presented a method that combines histogram-shifting and difference expansion reversible data hiding.

Chang et al. [2] proposed dual-image based data hiding technique using exploiting modification direction (EMD) method. They first established a (256×256) modulus function magic matrix. In their scheme, a binary secret message is first converted into secret digits in the base-5 numeral system. Then, two secret digits are taken to embed into a pixel pair at a time by embedding each secret digit into each steganographic image. Lee et al. [7] introduced a lossless steganographic technique that utilized centralized difference expansion to hide more secret data into smoother areas of host image. Later, Lee et al. [12] embed secret data using the four directions of the center point of pixels to obtain the stego-pixels of the two images. Lee and Huang [11] converted secret data into

quinary-based secret symbols and combined every two secret symbols as a set for embedding. Qin et al. [18] embedded the first image using EMD, and the second image through three rules which were dependent on the first image. Lu et al. [14] used the least-significant-bit (LSB) matching method for embedding. They obtained the stego-pixels of two images through the modulus function and the LSB, checked whether the stego-pixels are reversible via an averaging method, and then modified the non-reversible stego-pixels based on a rule table to successfully restored the image. Lee et al. [12] embedded secret data using directions to achieve high image quality, but the embedding capacity could only reach 0.75 bits per pixel (bpp). Chang et al. [2] embed secret data through the modulus function matrix to achieve a higher capacity that is 1.00 bpp, but image quality was inferior to that using the method by Lee et al. Thus, the challenge to enhance embedding capacity while maintaining high image quality through the use of dual-image techniques is still an important issue.

In this paper, we introduced a new dual-image based reversible data hiding scheme through Pixel Value Difference Expansion (PVDE).

- Our motivation is to enhance the embedding capacity and achieve reversibility in data hiding. Data embedding using PVD was not reversible. We have applied DE data embedding scheme to keep the distance parameter of sub range of reference table within the pixel pair. The lower bound of sub range of reference table help us to achieve reversibility in PVDE. The proposed scheme also enhance embedding capacity.

- One of the important modification that we have propose in our scheme is uniform sub range in the reference table. In PVD, the width of sub range varies and the number of embedding bits depends on the pixel value difference. More number of data bits are embedded in the complex area of an image which will effect more. To maintain the uniform effect after data embedding in all area, we propose uniform width of sub range in the reference table. Although data could be embedded without reference table, we use reference table to make PVD as reversible. The lower label of sub range in each embedding pair is essential for PVD to recover original image.

- Another motivation is to enhance security in data hiding. We distribute modified pixel pair among dual stego image, stego major (SM) and stego auxiliary (SA) based on shared secret key bit stream. The secret message bits are distributed among dual image. The receiver applies extraction technique using either PVD or DE that depends on the share secret key. Without key none can extract secret message. Finally, we recover original image using our extraction algorithm from dual image without any distortion.

The rest of the paper is organized as follows. Section 2 describes some preliminary techniques of data hiding scheme. Proposed data hiding scheme PVDE in detail is discussed in Section 3. The issue regarding overflow and underflow situation are described in Section 4. Experimental results with comparisons are discussed in Section 5. Section 6 present security analysis. Finally, we conclude our paper with some interesting insights and possible future directions in Section 7.

2 Preliminaries

Reversible data hiding become a very important and challenging task in hidden data communication specially in medical and military application for ownership identification, authentication and copy right protection. We propose dual-image based reversible data hiding scheme called PVDE. In this section, Wu and Tsai's PVD and Tian's DE techniques are discussed briefly.

2.1 Wu and Tsai's Scheme

Pixel Value Differencing (PVD), proposed by Wu and Tsai [26] is one of the popular data hiding techniques in spatial domain. Consider a two consecutive pixels P_x and P_{x+1} from cover image C of size $(M \times N)$. The difference value d of P_x and P_{x+1} can be derived by

$$d = |P_x - P_{x+1}|.$$

A reference table R is used which consists of n contiguous sub-blocks with fixed interval. The main function of the reference table is to provide data hiding information. Each sub-range has its lower bound (lb) and upper bound (ub) values and the width w of each sub-range is selected to be a power of 2. The hiding capacity of two consecutive pixels can be obtained by

$$t = \lfloor log_2\ w \rfloor. \tag{1}$$

Here, t is the number of bits that is hidden within pixel pair. A new parameter $d^{'}$ is generated using

$$d^{'} = m_1 + lb.$$

Now the secret data is embedded into pixel pair (P_x, P_{x+1}) by modifying it such that d and $d^{'}$ belongs to the same range in the reference table. The details of the embedding criteria are as follows:

$$(P_x^{'}, P_{x+1}^{'}) = \begin{cases} (P_x + \lceil d^{''}/2 \rceil, P_{x+1} - \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x \geq P_{x+1} \text{ and} & d^{'} > d; \\ (P_x - \lceil d^{''}/2 \rceil, P_{x+1} + \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x < P_{x+1} \text{ and} & d^{'} > d; \\ (P_x - \lceil d^{''}/2 \rceil, P_{x+1} + \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x \geq P_{x+1} \text{ and} & d^{'} \leq d; \\ (P_x + \lceil d^{''}/2 \rceil, P_{x+1} - \lfloor d^{''}/2 \rfloor), & \\ \text{if } P_x < P_{x+1} \text{ and} & d^{'} \leq d; \end{cases}$$

where $d^{''} = |d^{'} - d|$. An illustration of how $P_x^{'}$ and $P_{x+1}^{'}$ can be adjusted by Wu and Tsai 's scheme for the purpose of hiding secret data is shown in Figure 1. The recovery

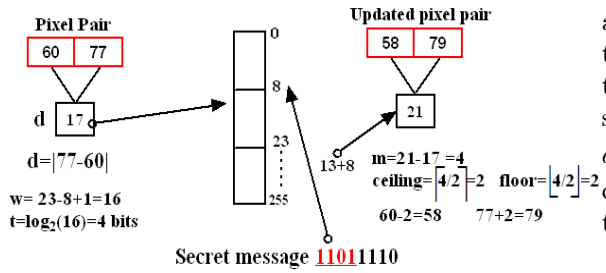

Figure 1: Data embedding through PVD with example

process of Wu and Tsai 's method is quite simple and easy. Given two consecutive pixels $P_x^{'}$ and $P_{x+1}^{'}$ of the stego image, we compute their difference value $d^{'}$ and obtain $d^{'}$=$|P_{x+1}^{'}$ - $P_x^{'}|$. Then we use the original reference table R in the embedding phase to obtain the same sub range. The length t of the hiding capacity can also be gained by using Equation (1). Then we extract message $m_1 = d^{'}$ - lb and convert the decimal value m_1 into a binary string whose length is t bits. For example, in Figure 1, m_1= $21-8=(13)_{10}$ and $t=4$, and then secret data $(1101)_2$ is extracted.

2.2 Tian 's Scheme

Tian [22] presented a reversible data hiding technique based on a difference expansion for gray-scale images. Consider a pixel pair of cover image P_x and P_{x+1}. After embedding 4 bits secret data using PVD, we obtained modified pixel $P_x^{'}$ and $P_{x+1}^{'}$. For embedding secret data within consecutive pixel pair $P_x^{'}$ and $P_{x+1}^{'}$, where $0\leq$ ($P_x^{'}$, $P_{x+1}^{'}$) ≤ 255 the following process is discussed. The average value A and the difference value d is computed by

$$A=\lfloor\frac{P_x^{'}+P_{x+1}^{'}}{2}\rfloor,\ d=|P_x^{'}-P_{x+1}^{'}|. \quad (2)$$

The inverse integer transform of Equation (2) is

$$P_x^{'}=A+\lfloor\frac{d+1}{2}\rfloor, P_{x+1}^{'}=A-\lfloor\frac{d}{2}\rfloor. \quad (3)$$

Such a transform in Equation (2) and Equation (3) are called integer Haar wavelet transform or S transform. Obviously, the transform is a one-to-one correspondence between ($P_x^{'}$, $P_{x+1}^{'}$) and (A,d). That means, it meets the requirement of reversibility. Tian expands the difference twice for vacate a space and embed a secret bit s, where $s\in\{0,1\}$ is the binary secret and generates a new difference value $d^{'}$ by

$$d^{'}=2\times d+s.$$

The new pixel values $P_x^{''}$ and $P_{x+1}^{''}$ are obtained by

$$(P_x^{''},P_{x+1}^{''})=(A+\lfloor\frac{d^{'}+1}{2}\rfloor, A-\lfloor\frac{d^{'}}{2}\rfloor).$$

Finally, the embedding operation is completed, and it produces a stego-image pixel pair by modifying ($P_x^{'}$ and $P_{x+1}^{'}$) to ($P_x^{''}$ and $P_{x+1}^{''}$). Figure 2 is the illustration of Tian's difference expansion scheme. During extraction the secret message, the difference value of consecutive pixel pair ($P_x^{''}$, $P_{x+1}^{''}$) is obtained by calculating $d^{'}=|P_x^{''}-P_{x+1}^{''}|$. The secret bit s can be extracted by computing $s=d^{'}\ mod\ 2$. Then, the average value A and the original difference value d are obtained by

$$A^{'} = \lfloor\frac{P_x^{''}+P_{x+1}^{''}}{2}\rfloor$$
$$d = \lfloor\frac{d^{'}}{2}\rfloor.$$

Now, the original pixel values are recovered using

$$(P_x^{'},P_{x+1}^{'})=(A^{'}+\lfloor\frac{d+1}{2}\rfloor,\ A^{'}-\lfloor\frac{d}{2}\rfloor).$$

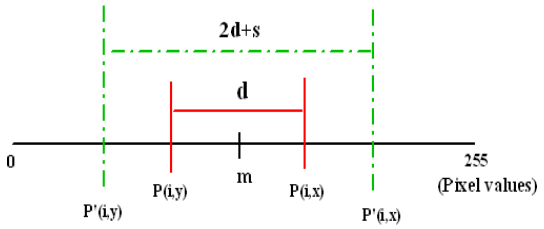

Figure 2: Difference expansion

3 Proposed PVDE Scheme

In this paper, we propose a new reversible data hiding scheme by combining Pixel Value Difference (PVD) and Difference Expansion (DE) on dual image called PVDE. According to this approach, first we have to select two consecutive pixels x_i and x_{i+1} from cover image C. Then we calculate the pixel value difference d between x_i and x_{i+1} that is

$$d=|x_i-x_{i+1}|.$$

The number of secret bits which will be embedded in the cover image is determined with the help of a reference table R. The reference table have equal sub range $[lb,ub]$ having length w that is $w=ub-lb+1$. In our proposed PVDE scheme, w is taken as 16. Hence forth the contiguous sub-ranges are $\{0-15,\ 16-31,\ 32-47,\ \ldots,\ 240-255\}$ which have capability to embed 4 secret bits within each pixel pair through PVDE in cover image. Now to embed 4 bits, two new parameters $d^{'}$ and $d^{''}$ are introduced as follows:

$$d^{'} = lb+m_1$$
$$d^{''} = d^{'}-d$$

where m_1 is decimal value of the secret message of size 4 bits. After that the pixel values x_i and x_{i+1} are adjusted into two new pixel values $x_i^{'}$ and $x_{i+1}^{'}$ by following

modifications.

$$\begin{aligned} x_i^{'} &= x_i - \delta \\ x_{i+1}^{'} &= x_{i+1} + \gamma \end{aligned}$$

where $\delta = \lceil \frac{d^{''}}{2} \rceil$ and $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$. Then we apply DE on the pixels $x_i^{'}$ and $x_{i+1}^{'}$ to embed one bit. Now, we determine the lower range from the reference table R where the difference d belongs to. Then we calculate the parameters h, A and $h^{'}$ as follows

$$\begin{aligned} h &= (d - lb) \\ A &= (x_i^{'} + x_{i+1}^{'})/2 \\ h^{'} &= (2 \times h + m_2) \end{aligned}$$

where m_2 is one bit secret message. After this the pixel pair $x_i^{'}$ and $x_{i+1}^{'}$ are again modified by

$$\begin{aligned} x_i^{''} &= A + \delta_1 \\ x_{i+1}^{''} &= A - \gamma_1 \end{aligned}$$

where $\delta_1 = \lceil (h^{'}/2) \rceil$ and $\gamma_1 = \lfloor (h^{'}/2) \rfloor$. Finally, the stego pixel pairs $(x_i^{'}, x_{i+1}^{'})$ and $(x_i^{''}, x_{i+1}^{''})$ are distributed among dual stego image, Stego Major (SM) and Stego Auxiliary (SA) based on shared secret key K. If $K = 1$, then the pixel pair $(x_i^{'}, x_{i+1}^{'})$ is stored within the stego image SM and the pixel pair $(x_i^{''}, x_{i+1}^{''})$ is stored within the stego image SA. Again if $K = 0$ then the pixel pair $(x_i^{'}, x_{i+1}^{'})$ is stored within the stego image SA and the pixel pair $(x_i^{''}, x_{i+1}^{''})$ is stored within the stego image SM. The detailed schematic diagram of our proposed PVDE method for embedding process are shown in Figure 3 and the corresponding algorithm is shown in Algorithm 1.

Algorithm 1: Data embedding of PVDE

Input: Original image I ($M \times N$), Secret message M, Shared secret key K.
Output: Two stego images, Stego Major (SM) and Stego Auxiliary (SA) of size ($M \times N$).

1: Select pixel pair (x_i, x_{i+1}) from I in raster scan order;
2: Calculate difference $d = |x_i - x_{i+1}|$;
3: Select 4 bits secret message from M and convert into decimal value m_1 and 1 bit as m_2;
4: Calculate $d^{'} = m_1 + lb$; where, lb is the lower bound of the sub range of reference table R in which d belongs to;
5: Calculate $d^{''} = d^{'} - d$;
6: Compute $\delta = \lceil \frac{d^{''}}{2} \rceil$ and $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$;
7: **if** $(x_i > x_{i+1})$ **then**
8: $x_i^{'} = x_i + \gamma$; $x_{i+1}^{'} = x_{i+1} - \delta$;
9: **else**
10: $x_i^{'} = x_i - \delta$; $x_{i+1}^{'} = x_{i+1} + \gamma$;
11: **end if**
12: Calculate $h = (d - lb)$;

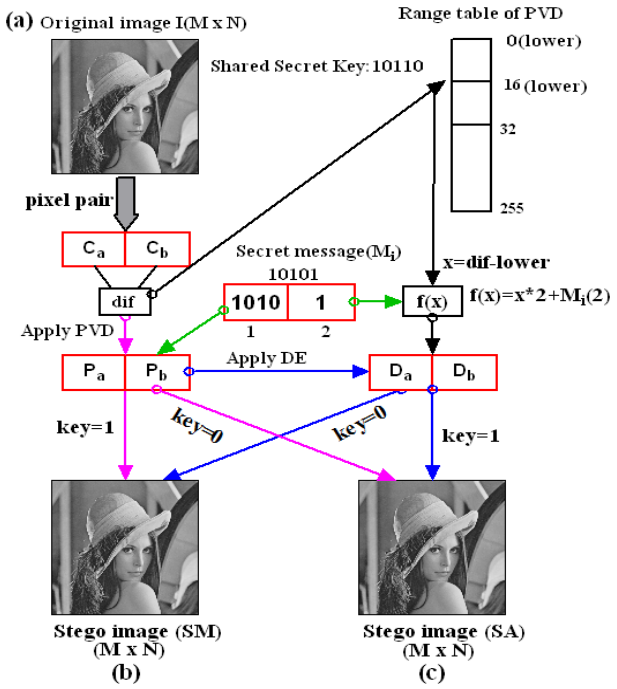

Figure 3: Schematic diagram of PVDE for data embedding process

13: Calculate $h^{'} = 2 \times h + m_2$; where, m_2 is 1 bit secret message;
14: Calculate Average $A = \lfloor \frac{(x_i^{'} + x_{i+1}^{'})}{2} \rfloor$;
15: Calculate $\delta_1 = \lceil \frac{h^{'}}{2} \rceil$; and $\gamma_1 = \lfloor \frac{h^{'}}{2} \rfloor$;
16: **if** $(x_i^{'} > x_{i+1}^{'})$ **then**
17: $x_i^{''} = A + \delta_1$; $x_{i+1}^{''} = A - \gamma_1$;
18: **else**
19: $x_i^{''} = A - \gamma_1$; $x_{i+1}^{''} = A + \delta_1$;
20: **end if**
21: **if** $(K = 1)$ **then**
22: Store $(x_i^{'}, x_{i+1}^{'})$ within stego image SM and store $(x_i^{''}, x_{i+1}^{''})$ within stego image SA;
23: **else**
24: Store $(x_i^{'}, x_{i+1}^{'})$ within stego image SA and store $(x_i^{''}, x_{i+1}^{''})$ within stego image SM;
25: Repeat **Line-1** through **Line-24** until $length(M) = 0$;
26: Dual stego image SM and SA are generated;
27: **end if**
28: End

At the receiver end, both the data extraction and original image reconstruction are performed by taking pixel from both the stego images SM and SA based on K. If $K = 1$, then select pixel pair $(x_i^{'}, x_{i+1}^{'})$ from SM and apply data extraction using PVD and at the same time select pixel pair $(x_i^{''}, x_{i+1}^{''})$ from SA and apply data extraction using DE. If $K = 0$, then apply the pixel pair selection process opposite manner, that means select pixel pair $(x_i^{'}, x_{i+1}^{'})$ from stego image SA and $(x_i^{''}, x_{i+1}^{''})$ from

stego image SM. Now the data extraction and original image reconstruction process are described as follows:

$$\begin{aligned} d &= |x_i^{'} - x_{i+1}^{'}| \\ m_1 &= d - lb \end{aligned}$$

where lb is the lower bound of the sub range of the reference table R to which d belongs to and m_1 is the 4 bits secret data. To recover another secret bit, we perform

$$h^{'} = x_i^{''} - x_{i+1}^{''}$$

and collect one bit secret message (m_2) from LSB of $h^{'}$. To recover the original image, we perform the following calculations

$$\begin{aligned} h &= \lfloor \frac{h^{'}}{2} \rfloor \\ d^{'} &= (h + lb) \\ d^{''} &= d^{'} - d \\ \delta &= \lceil \frac{d^{''}}{2} \rceil \\ \gamma &= \lfloor \frac{d^{''}}{2} \rfloor. \end{aligned}$$

Now, the original image pixel (x_i, x_{i+1}) is recovered by

$$(x_i, x_{i+1}) = \begin{cases} x_i^{'} - \gamma,\ x_{i+1}^{'} + \delta & \text{if } x_i^{'} > x_{i+1}^{'} \\ x_i^{'} + \delta,\ x_{i+1}^{'} - \gamma & \text{otherwise} \end{cases}$$

The extraction process of our proposed PVDE scheme is explained using a schematic diagram in Figure 4. The corresponding algorithm for data extraction and original image reconstruction is explained in Algorithm 2.

Algorithm 2: Data extraction of PVDE

Input: Two stego images SM and SA, Shared secret key K.

Output: Original Image $I(M \times N)$; Secret Message M;

1: Select pixel pair from SM and SA in raster scan order;
2: **if** $(K = 1)$ **then**
3: Collect $(x_i^{'}, x_{i+1}^{'})$ from SM and collect $(x_i^{''}, x_{i+1}^{''})$ from SA;
4: **else**
5: Collect $(x_i^{'}, x_{i+1}^{'})$ from SA and collect$(x_i^{''}, x_{i+1}^{''})$ from SM;
6: **end if**
7: Calculate $d^{'} = |x_i^{'} - x_{i+1}^{'}|$;
8: Secret message $m_1 = d^{'} - lb$, where lb is the lower bound of the sub range of range table R;
9: Calculate $h^{'} = (x_i^{''} - x_{i+1}^{''})$; (Extract secret message bit m_2 from LSB of $h^{'}$);
10: Calculate $h = \lfloor \frac{h^{'}}{2} \rfloor$;
11: Calculate $d = (h + lb)$; where lb is the lower bound of the sub range of the reference table R in which d belongs;

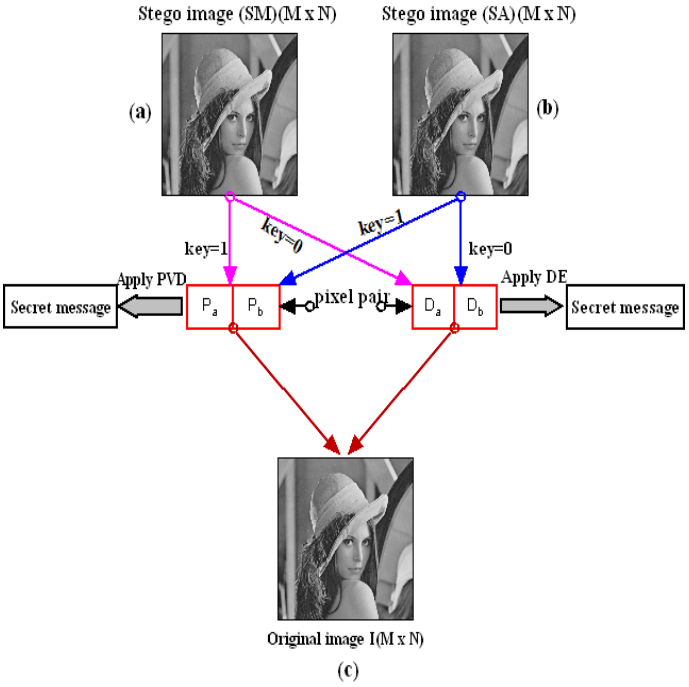

Figure 4: Schematic diagram of PVDE for data extraction process

12: Calculate $d^{''} = d^{'} - d$;
13: Calculate $\delta = \lceil \frac{d^{''}}{2} \rceil$;
14: Calculate $\gamma = \lfloor \frac{d^{''}}{2} \rfloor$;
15: **if** $(x_i^{'} > x_{i+1}^{'})$ **then**
16: $x_i = x_i^{'} - \gamma$; $x_{i+1} = x_{i+1}^{'} + \delta$;
17: **else**
18: $x_i = x_i^{'} + \delta$; $x_{i+1} = x_{i+1}^{'} - \gamma$;
19: **end if**
20: Repeat **Line-1** through **Step-19** until all data are extracted;
21: End

4 Overflow and Underflow

When the stego pixel value cross the upper range of gray scale then overflow occur and cross the lower limit of gray scale then underflow occur. We have use 8 bit image where gray scale is [0-255]. Suppose we have a pixel pair (C_a, C_b) with pixel values $C_a = 250$ and $C_b = 255$ and 4 bits secret data is $(1101)_2$ that is $(13)_{10}$. The difference between two pixels d is $|\ 250 - 255\ |$=5 and the new difference $d^{'}$ is 13+0=13. Therefore, m =13-5=8, c=4 and f=4. After embedding, the stego pixel pair becomes $P_a = 246$ and $P_b = 259$ which cross the upper limit that means $P_b > 255$ which shows overflow problem.

For underflow, suppose C_a=0 and C_b=7 and 4 bits secret data is $(1010)_2$ that is $(10)_{10}$. The difference between two pixels d is $|\ 0 - 7\ |$=7 and the new difference $d^{'}$ is 10+0=10. Therefore, m =10-7=3, c=2 and f=1. The

stego pixel pair becomes $P_a = -2$ and $P_b = 8$. We observe that $P_a < 0$ which shows underflow problem.

To overcome this problem, we do not embed any secret data within those specified pixel pair. We observed that after data embedding, the difference between two pixels is not much more than 31. To overcome the overflow problem, we use difference expansion method and set the difference 32 when data hiding by difference expansion is 0 and subtracting 32 from the average of two pixels. So, the modified pixel pair becomes $(D_a = avg-32, D_b = P_b)$ and set the difference 33 when data is 1 by subtracting 33 from the average of two pixels. So, the modified pixel pair becomes $(D_a = avg - 33, D_b = P_b)$.

To overcome the underflow problem, we set the difference 32 when data is 0 by adding 32 with the average of two pixels. So, the modified pixel pair will be $(D_a = avg + 32, D_b = P_b)$ and set the difference 33 when data is 1 by adding 33 with the average of two pixels. So, the modified pixel pair will be $(D_a = avg + 33, D_b = P_b)$.

In the receiver side, when difference between the pixels D_a and D_b is 32 or 33 the receiver understand that secret message is not embedded within that pair (P_a, P_b) corresponding to (D_a, D_b).

Figure 5: Standard test images with (256×256) pixel

5 Experimental Results and Comparison

In this section, our proposed method (PVDE) is verified and tested using gray scale image of size (256×256) pixels collected from [25] shown in Figure 5. After embedding the secret messages, dual stego image, Stego Major (SM) and Stego Auxiliary (SA) are generated as shown in Figure 6. Our developed algorithms: PVDE embedding and extraction are implemented in MATLAB Version 7.6.0.324 (R2008a). Here, the distortion is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio $(PSNR)$. The MSE is calculated as follows:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2}{(M \times N)}$$

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image respectively.

Figure 6: Dual stego images of (256×256) pixels after data embedding

$X(i,j)$ represents the pixels in the cover image and $Y(i,j)$ represents the pixels of the stego image. The difference between the original and stego images were assessed by the Peak Signal to Noise Ratio $(PSNR)$. The formula of PSNR is as follows:

$$PSNR = 10\ log_{10}\frac{255^2}{MSE}$$

Table 1: Data embedding capacity with PSNR

Image	Data(bits)	PSNR(SM)	PSNR(SA)	Avg. PSNR
cameraman	40,000	43.40	42.72	36.77
	80,000	35.75	38.84	
	1,60,000	30.77	36.19	
	1,63,592	30.35	36.14	
house	40,000	47.00	41.88	38.95
	80,000	40.59	38.53	
	1,60,000	35.84	36.01	
	1,63,592	35.79	35.97	
F16	40,000	47.07	43.29	37.88
	80,000	37.18	39.36	
	1,60,000	31.65	36.48	
	1,63,592	31.62	36.41	
lake	40,000	36.95	43.15	36.08
	80,000	33.47	39.70	
	1,60,000	30.82	37.03	
	1,63,592	30.63	36.93	
Lena	40,000	40.31	43.78	36.93
	80,000	35.31	40.19	
	1,60,000	30.77	37.28	
	1,63,592	30.67	37.18	
livingroom	40,000	38.93	43.47	36.69
	80,000	34.18	40.02	
	1,60,000	31.37	37.19	
	1,63,592	31.31	37.11	
peppers	40,000	39.67	43.47	37.27
	80,000	35.45	39.93	
	1,60,000	32.92	36.98	
	1,63,592	32.86	36.89	
pirate	40,000	39.79	43.75	37.05
	80,000	35.29	40.28	
	1,60,000	31.58	37.15	
	1,63,592	31.48	37.09	
bridge	40,000	34.57	43.54	35.85
	80,000	32.39	40.47	
	1,60,000	30.50	37.51	
	1,63,592	30.44	37.42	
Tiffany	40,000	40.44	43.75	37.36
	80,000	36.32	40.20	
	1,60,000	32.00	37.19	
	1,63,592	31.92	37.12	
Zelda	40,000	42.20	43.76	38.87
	80,000	39.10	40.09	
	1,60,000	36.08	36.98	
	1,63,592	35.86	36.90	
Goldhill	40,000	45.84	42.85	38.66
	80,000	39.77	39.48	
	1,60,000	34.09	36.80	
	1,63,592	34.06	36.76	

Higher the values of PSNR between two images indicates better the quality of the stego image and very similar to the cover image where as low PSNR demonstrates the opposit. Table 1 shows the experimental result upon Cameraman, House, Jet Plane, Lake, Lena, Living Room, Peppers, Pirate, Walk bridge and Woman images. Table 1 shows the average $PSNR$ of SM and SA with cover image. To asses the embedding capacity, we calculate payload (B) in terms of bits per pixel (bpp) using the following expression.

$$B = \frac{(\lfloor \frac{M}{2} \rfloor - 1) \times N \times 5}{(2M \times 2N)}$$

For example, if $M = 512$ and $N = 512$ then $B = \frac{255 \times 512 \times 5}{2 \times (512 \times 512)} = 1.25$. The bpp B of our dual image based PVDE scheme is 1.25.

To measure the complexity, we assume that the size of the cover image is $(M \times N)$ and the data embedding process embed five secret bits within a pixel pair. Two copies of cover image is used to distribute the stego pixel and each pixel pair from cover image produce two copies of pixel pair. So, the time complexity is O(MN). On the other hand, during data extraction, we need to scan the pixel pair from dual image depending on key. So, the time complexity is O($2MN$).

Table 2 lists the average PSNR values with payload of different existing dual image based data hiding scheme. The average PSNR of the stego images of the proposed scheme is lower than the method proposed by Qin et al.'s [18], Lu et al.'s [14, 15], Chang et al.'s [2, 3] and Lee et al.'s [11, 12] schemes. But the average PSNR is higher than the method proposed by Lee et al.'s [10] and Zeng et al.'s [27] schemes. The embedding payload of our scheme is 1.25 bpp which is higher than the other existing dual image based schemes. The embedding payload of the methods proposed by Qin et al. [18] is approximately 0.09 bpp less than that of our proposed PVDE method. The payload of Lu et al. [15] and Chang et al. [2, 3] is approximately 0.25 bpp less than our PVDE method. It is observed that our PVDE is superior than the other dual image based schemes in terms of embedding payload (bpp). From the above discussion, one can conclude that PVDE is better than other existing scheme in terms of payload, and the PSNR is also reasonable which implies the quality of the stego image is good.

Table 2: Comparison of average PSNR and payload (bpp) with existing schemes

Scheme	Avg. PSNR (dB)	Capacity (bpp)
Chang et al.(2007)	45.1225	1.00
Chang et al.(2009)	48.14	1.00
Lee et al. (2009)	52.3098	0.74
Lee et al. (2010)	34.38	0.91
Zeng et al. (2012)	32.74	1.04
Lee and Huang (2013)	49.6110	1.07
Qin et. al. (2014)	52.11	1.16
Lu et al. (2015)	49.20	1.00
Proposed PVDE	38.95	1.25

6 Steganalysis

Steganalysis is the art of discovering whether or not a secret message is exist in a suspected image. Steganalysis does not however consider the successful extraction of the message. Now a days, steganographic systems does not achieve perfect security. So, they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not. Steganalyst perform this work in various ways. The way is divided into two main categories-Targeted and Blind steganalysis. Some of the targeted steganalysis are visual attack, statistical attack and structural attack and one of the famous blind steganalysis method is RS analysis.

6.1 RS Analysis

We analyzes our stego images by RS analysis [4]. Let us assume that we have a cover image of size (M × N). In RS analysis method, first the stego image is divide into disjoint groups G of n adjacent pixels $(x_1, \ldots, x_n)$. Each pixel value is in a set P that is $p = \{0, 1, \ldots, 255\}$. Here, each group consist of 4 consecutive pixels in a row. Define a discrimination function f that returns a real number $f(x_1, \ldots, x_n) \in R$ to each pixel group $G = (x_1, \ldots, x_n)$. The main goal of use the discrimination function is to identify the "Smoothness" or "Regularity" of each group of pixels G. The discrimination function f is define as:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

An invertible function F is define which is operates on P, called "flipping". Flipping consists of two-cycles which permutes the pixels value. So, F^2= Identity or $F(F(x)) = x$ for all x belongs to P. Flipping the LSB of each pixel value and the corresponding permutation F1 is: $0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$. Define another function, named shift LSB flipping and treated as F_{-1}. So the permutation F_{-1}: $-1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256$. In the other word, F_{-1} flipping can be define as:

$$F_{-1}(x) = F_1(x + 1) - 1, \quad \text{for all } x.$$

There are three types of groups Regular groups (R), Singular groups (S) and Unusable groups (U) which are define depend on the discrimination function f and the flipping operation F. Depending on the condition groups are define below.

$$\begin{cases} G \in R & \text{if } f(F(G)) > f(G) \\ G \in S & \text{if } f(F(G)) < f(G) \\ G \in U & \text{if } f(F(G)) = f(G) \end{cases}$$

where $F(G) = F(x_1), \ldots, F(x_n)$.
The flipping operation will be execute with the help of a mask value M, which is a n tuples with values -1, 0, and 1. The flipped group $F_M(G)$ is defined as $(F_M(1)(x1)$, $F_M(2)(x2)$, ..., $F_M(n)(xn))$. The RS analysis based on analyzing how the number of regular and singular groups changes with the increased message length embedded in the LSB plane.

Then calculate the value of RS analysis using the following equation.

$$((|R_M - R_{-M}| + |S_M - S_{-M}|)/(R_M + S_M))$$

where R_M and R_{-M} is the total number of regular group with mask M and -M respectively. S_M and S_{-M} is the total number of singular group with mask M and -M respectively. When the value of RS analysis is closed to zero means the scheme is secure. The stego images are tested under the RS analysis. It is observed from Tables 3 and 4 that the values of R_M and R_{-M}, S_M and S_{-M} are nearly equal for stego image SM and SA. Thus rule $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ is satisfied for the stego image in our scheme. So, the proposed method is secure against RS attack. In our experiment, the ration of R and S lies between 0.0051 to 0.0616 for SM and 0.0043 to 0.0267 for SA of Cameraman image.

Table 3: RS analysis of PVDE method (Stego image SM)

Image	Data	SM				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	20000	7118	7107	3551	3594	0.0051
	50000	6768	6851	3944	3895	0.0123
	75000	6304	5947	4943	5279	0.0616
	114582	6207	6035	4997	5173	0.0311
Lena	20000	5617	5607	4067	4068	0.0011
	50000	5563	5476	4291	4337	0.0135
	75000	5636	5539	4517	4589	0.0166
	114582	5641	5387	4509	4709	0.0447
Baboon	20000	5893	5815	4960	5105	0.0205
	50000	5897	5875	5076	5131	0.0070
	75000	6018	5813	5107	5313	0.0369
	114582	5844	5986	5256	5123	0.0248

Table 4: RS analysis of PVDE method (Stego image SA)

Image	Data	SA				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	20000	6945	7078	3877	3721	0.0267
	50000	6506	6535	4490	4472	0.0043
	75000	6514	6528	4287	4224	0.0071
	114582	6538	6647	4283	4225	0.0154
Lena	20000	5575	5565	4139	4133	0.0016
	50000	5590	5514	4239	4299	0.0138
	75000	5587	5442	4579	4665	0.0227
	114582	5652	5621	4592	4553	0.0123
Baboon	20000	5876	5881	4995	5092	0.0094
	50000	5821	5878	5121	5147	0.0076
	75000	5895	5827	5196	5283	0.0140
	114582	5874	5830	5194	5206	0.0051

6.2 Relative Entropy

To measure the security in our proposed method, the relative entropy (D) between the probability distributions of the original image (P) and the stego image (Q) is calculated by

$$D(Q||P) = \sum q(x) log \frac{q(x)}{p(x)}.$$

When relative entropy between two probability distribution functions is zero then the system is perfectly secure. D($Q||P$) is a nonnegative continuous function and equals to zero if and only if p and q are coincide. Thus D($Q||P$) can be normally considered as a distance between the measures p and q. Relative entropy of the probability distribution of the original image and the stego image varies depending upon number of bits of secret message. In our experiment, it is shown that when the number of characters in the secret message increases, the relative entropy in stego image is also increases. The relative entropy in our experiment is varies between 0.0027 to 0.0131 for lena image which implies the proposed scheme provides

Table 5: Relative entropy between I and SM

Image	Data(Bytes)	Entropy I	Entropy SM	Difference
Lena	5000	7.4451	7.4451	0.0027
	10000	7.4451	7.4452	0.0058
	20000	7.4451	7.4452	0.0105
	20249	7.4451	7.4453	0.0131
Barbara	5000	7.0480	7.0480	0.0031
	10000	7.0480	7.0482	0.0064
	20000	7.0480	7.0485	0.0112
	20249	7.0480	7.0486	0.0134
Tiffany	5000	7.2925	7.2925	0.0029
	10000	7.2925	7.2925	0.0057
	20000	7.2925	7.2926	0.0122
	20249	7.2925	7.2926	0.0129
Pepper	5000	7.2767	7.2767	0.0039
	10000	7.2767	7.2768	0.0077
	20000	7.2767	7.2770	0.0142
	20249	7.2767	7.2771	0.0169
Gold hill	5000	7.2367	7.2367	0.0034
	10000	7.2367	7.2371	0.0056
	20000	7.2367	7.2375	0.0112
	20249	7.2367	7.2379	0.0143

secure hidden communication. Other relative entropy values with SM are depicted in Table 5.

6.3 Histogram Attack

Figure 7 depicted the histogram of the cover and stego image and their difference histogram are obtained. The stego image are produced from cover image employing the maximum data hiding capacity. It is observed that the shape of the histogram is preserved after embedding the secret data. Histogram of cover image is represented as h whereas histogram of stego image is represented as $h^{'}$. The change of histogram can be measured by

$$D_h = \sum_{m=1}^{255} |h_m^{'} - h_m|.$$

The difference of the histogram is very small. It is observed that, bins close to zero are more in numbers and the bins which are away from zero are less in numbers. This confirm the quality of stego image. There is no step pattern observed which ensure the proposed method is robust against histogram analysis.

6.4 Statistical Attack

The proposed scheme is also assessed based on statistical distortion analysis by some image parameters like Standard Deviation (SD) and Correlation Coefficient (CC) to check the impact on image after data embedding. The SD before and after data embedding and CC of cover and stego images are summarized in Table 6. Minimizing parameters difference is one of the primary aims in order to get rid of statistical attacks. From the Table 6 it is seen that there is no substantial divergence between the SD of the cover-image and the stego-image. This study shows that the magnitude of change in stego-image based on image parameters is small from a cover image. Since the image parameters have not changed much, the method

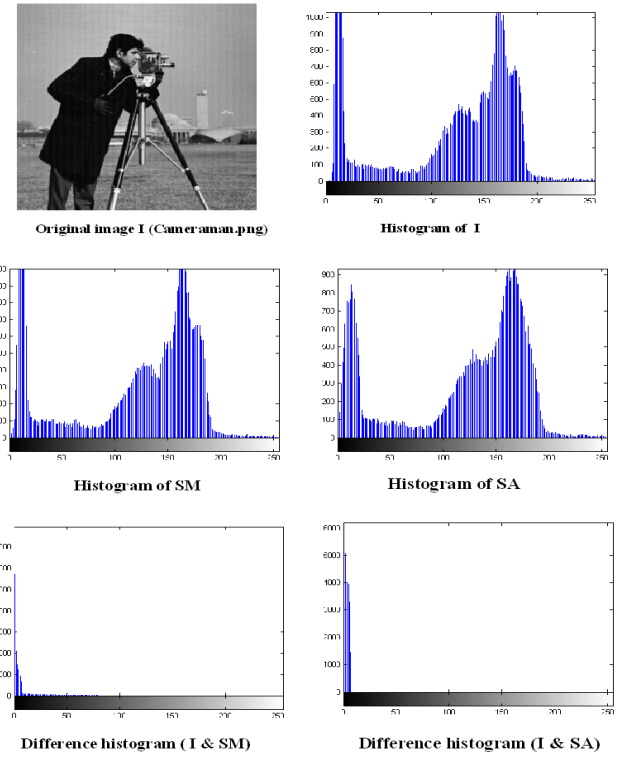

Figure 7: Histogram of Original, SM, SA and difference

Table 6: Standard Deviation (SD) and Correlation Coefficient (CC)

Image	SD			CC		
	I	SM	SA	I&SM	I&SA	SM & SA
Baboon	38.37	37.85	38.54	0.98	0.99	0.97
Cameraman	61.59	61.12	61.73	0.99	0.99	0.99
Lena	47.83	47.43	47.97	0.98	0.99	0.98

offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates a perfectly secure steganographic system.

6.5 Attacks with Unknown Secret Key

We have used 128 bits shared secret key K to distribute pixel among dual images. The scheme is secure to prevent possible malicious attacks. The proposed scheme constructs two stego images which protect original information by hiding secret information in both images SM and SA. The Figure 8 shows the revelation example where with key and without key stego images are used to revel the hidden message. If the malicious attacker holds the original image and dual images and is fully aware of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct secret key. The result indicate that the attacker only acquires noise -like images when applying incorrect secret key to reveal the hidden message. Furthermore, the attacker may employ the brute force attack that tries all possible permu-

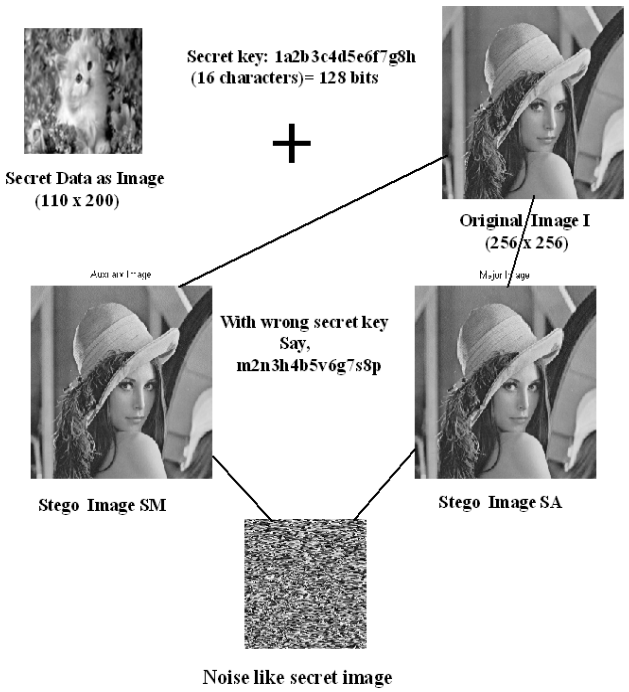

Figure 8: Noise like secret data with wrong secret key

tation to reveal the hidden message. The secret key are 128 bits length, so, the number of required trials to reveal the hidden message are 2^{128} which are computationally infeasible for current computers. The proposed scheme achieve stronger robustness against several attacks when compared with existing data hiding. Furthermore, the secret information can be retrieved without encountering any loss of data and recovered original image successfully from dual image.

7 Conclusion

In this paper, on the basis of pixel value difference and difference expansion a dual image based reversible data hiding scheme (PVDE) is introduced. Here, the reference table is modified allowing fix size four bits data embedding capacity. During difference expansion we keep the difference value of a subrange from the reference table which helps to recover the original image from stego images. In our proposed PVDE method, PVD achieved reversibility which demands the originality of our method. Also PVDE achieves security using the shared secret key by which stego pixels are distributed among two stego images. A shared secret key K has been used which guarantees security. The RS analysis provide low value which fulfilled the art of steganography. The visual attacks are analyzed by histogram analysis and statistical attacks are performed by SD and CC which provide robustness against several attacks. Also, the scheme maintains low relative entropy. In addition, it gains good PSNRs and higher payload than other existing methods of dual image based data hiding.

References

[1] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[2] C. C. Chang, Y. C. Chou. "Reversible data hiding scheme using two steganographic images" in *IEEE Region 10 Conference on TENCON*, pp. 1–4, 2007.

[3] C. C. Chang, Y. C. Chou, and T. D. Kieu, "Information Hiding in Dual Images with Reversibility", *Proceedings of Third International Conference on Multimedia and Ubiquitous Engineering*, pp. 145–152, 2009.

[4] J. Fridrich, J. Goljan, R. Du, "Invertible authentication", in *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents*, vol. 4314, pp.197208, SanJose, CA, Jan. 2001.

[5] T. D. Kieu and C. C. Chang, "A steganographic scheme by fully exploiting modification directions", *Expert Systems with Applications*, vol. 38, pp. 10648–10657, 2011.

[6] H. J. Kim, C. Kim, Y. Choi, S. Wang, and X. Zhang, "Improved modification direction methods", *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 319–325, 2010.

[7] C. C. Lee, H. C. Wu, C. S. Tsai, Y. P. Chu, "Lossless Steganographic scheme with Centralized Difference Expansion", *Pattern Recognition*, vol. 41, pp. 2097–2106, 2008.

[8] C. F. Lee, C. C. Chang, P. Y. Pai, and C. M. Liu, "Adjustment hiding method based on exploiting modification direction", *International Journal of Network Security*, vol. 17, no. 5, pp. 607–618, 2015.

[9] C. F. Lee and H. L. Chen, "Adjustable prediction-based reversible data hiding", *Digital Signal Processing*, vol. 22, no. 6, pp. 941–953, 2012.

[10] C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion", *Journal of Systems and Software*, vol. 83, no. 10, pp. 1864–1872, 2010.

[11] C. F. Lee, Yu L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations", *Telecommunication Systems*, vol. 52, pp. 2237–2247, 2013.

[12] C. F. Lee, K. H. Wang, C. C. Chang, Y. L. Huang, "A reversible data hiding scheme based on dual steganographic images", in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, pp. 228–237, 2009.

[13] S. K. Lee, Y. H. Suh, Y. S. Ho, "Lossless data hiding based on histogram moification of difference images", in *Pacific Rim Conference on Multimedia*, LNCS 3333, pp. 340–347, Springer-Verlag, 2004.

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

[15] T. C. Lu, J. H. Wu, and C. C. Huang, "Dual-image-based reversible data hiding method using center folding strategy", *Signal Processing*, vol. 115, pp. 195–213, 2015.

[16] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[17] C. Qin, C. C. Chang, and Y. C. Chen, "Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism" *Signal Processing*, vol. 93, no. 9, pp. 2687–2695, 2013.

[18] C. Qin, C. C. Chang, and T. J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images" *Multimedia Tools and Applications*, pp. 1–12, 2014.

[19] C. Qin, C. C. Chang, Y. H. Huang, and Li T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109–1118, 2013.

[20] C. Qin, C. C. Chang, and Li T. Liao, "An adaptive prediction-error expansion oriented reversible information hiding scheme", *Pattern Recognition Letters*, vol. 33, no. 16, pp. 2166–2172, 2012.

[21] D. M. Thodi, J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking", *IEEE Translations on Image Processing*, vol. 16, no. 3, pp. 1057–7149, Mar. 2007.

[22] J. Tian, "Reversible data embedding using a difference expansion", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[23] Y. Yu Tsai, J. T. Chen, and C. S. Chan, "Exploring LSB substitution and pixel-value differencing for block-based adaptive data hiding", *International Journal of Network Security*, vol. 16, no. 5, pp. 359–364, 2014.

[24] H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding", *Information Sciences*, vol. 179, no. 14, pp. 2460–2469, 2009.

[25] University of Southern California, *The USC-SIPI Image Database*, Sept. 15, 2015. (`http://sipi.usc.edu/database/database.php`)

[26] D. Wu, W. Tsai, "A steganographic method for images by pixel-value differencing", *Pattern Recognition Letters*, vol. 24, pp. 1613–1626, 2003.

[27] X. T. Zeng, Z. Li, L. D. Ping, "Reversible data hiding scheme using reference pixel and multi-layer embedding", *AEU International Journal of Electron Communication*, vol. 66, no. 7, pp. 532–539, 2012.

Biswapati Jana is currently working as an Assistant Professor in the Department of Computer Science, Vidyasagar University, Paschim Medinipur, India. He received his B. Tech. and M. Tech. degrees in Computer Science and Engineering from University of Calcutta in 1999 and 2002 respectively. His research interests include Image Processing, Data Hiding and Steganography. He has published more than ten papers in National and International Conferences.

Dr. Debasis Giri did his masters (M.Tech and M.Sc) both from IIT Kharagpur, India and also completed Doctorate from IIT Kharagpur, India. He is ten-th all India rank holder in Graduate Aptitude Test in Engineering in 1999. He has published more than 25 papers in international journal/ conference. His current research interests include Cryptography, Information Security, E-commerce security and Design & Analysis of Algorithms. He is Editorial Board Member and Reviewer of many International Journals. He is also Program Committee Member of International Conferences. He is a life member of Cryptology Research Society of India.

Dr. Shyamal Kumar Mondal is currently Associate Professor in the Department of Applied Mathematics With Oceanology And Computer Programming, Vidyasagar University. He did his Ph.D. from Vidyasagar University in 2004, M.Tech from ISM, Dhanbad in 1999 and M.Sc from Vidyasagar University in 1994. His research interest include Operations Research, Meteorology, Fuzzy Set Theory, Soft Set Theory, Soft Computing and Data Hiding. He has published more than 50 papers in National and International Journals/Conferences.