Dual Image Based Reversible Data Hiding Scheme Using Weighted Matrix

Biswapati Jana
Department of Computer Science, Vidyasagar University
Midnapore, Pin-721102, India
(E-mail: biswapatijana@gmail.com)
(Received Sept. 9, 2015; revised and accepted May 12 & Aug. 1, 2016)

Abstract

In this paper, we introduce dual image based reversible data hiding scheme using weighted matrix. First, we partition the original image into (3×3) pixel blocks. Then we perform modulo sum of entry wise multiplication with a shared secret weighted matrix. We then calculate the difference between modulo sum value and secret message. According to the sign of this difference, we increase or decrease one at the corresponding pixel of image block and keep the position value by addition/subtraction with the original pixel. Repeat the same nine times to embed thirty six bits secret data within each pixel block. Finally, we distribute the original and stego pixel among dual image based on a shared secret key. At the receiver end, we successfully extract secret message using shared secret weighted matrix and shared secret key. Also we recover cover image without any distortion from dual stego image as because the original pixels are not effected during data embedding which assure reversibility. The proposed scheme provides average data embedding capacity 1.98 bits per pixel (bpp) with good visual quality measured by peak signal to noise ratio (PSNR) which are grater than 39 dB. We compare our scheme with other state-of-the-art methods and obtain reasonably better performance in terms of data embedding capacity.

Keywords: Dual Image; Reversible Data Hiding; RS Analysis; Steganographic Attack; Weighted Matrix

1 Introduction

The data hiding is a form of covered communication that usually puts stress on simply finding the presence of a secret message. The main intention of hidden data communication is to concentrate on precluding the adversary from moving out the content of the confidential message by applying a variety of distortions techniques. Thus, the imperceptibility becomes the most significant place for the data hiding schemes. A high embedding efficiency becomes the principal aim to accomplish for the current data hiding schemes by substituting the payload. Westfeld [27] proposed F5 algorithm that is an good example of this kind of scheme. In this scheme, matrix embedding is used based on Hamming codes to embed k-bits secret data by changing least significant bit in the cover work. The embedding efficiency gains with the increment of k, while the payload falls contrarily. In order to enhancing the embedding efficiency and payload at the same time, an extended F5 algorithm is proposed by Fan et al. [8]. A data hiding scheme for binary images, which uses a binary matrix and a weight matrix to enforce insertion, is mentioned by Tseng [23]. However, the embedding efficiency and payload cannot reach the best level when the scheme is used to deal with gray-scale image. Also the scheme was not reversible. Here, we propose high embedding reversible data hiding scheme using weighted matrix through dual image. In addition, a high-risk security vulnerability is exist because an attacker will be able to guess the form of weight matrix by using brute-force attack. In order to overcome the drawbacks of the previous schemes [8, 23], an improved embedding strategy is developed in this paper. We introduce shared secret key ξ to enhance the security and update weighted matrix for every new block by $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where gcd $(\kappa, 9) = 1$. The secret key ξ is required to distribute the updated pixel among dual image. The proposed scheme improve the embedding capacity and achieve reversibility.

1.1 Motivation

In this paper, we introduce a new dual image based reversible data hiding scheme using weighted matrix.

- Our main motivation is to enhance the embedding capacity, security and to achieve reversibility in data hiding. Data embedding schemes using weighted matrix was not reversible. We develop dual image based reversible data hiding scheme using weighted matrix.

- To enhance security we update weighted matrix for each new block. It is possible by using the update rule $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where gcd $(\kappa, 9) = 1$. Also, we use a shared secret key bit stream ξ to distribute original pixel and stego pixel among dual image.
- To enhance capacity, we use nine times modulo sum of entry wise multiplication with each block. In Li Fan et al.'s [7] scheme, only single sum of entry-wise multiplication is applied on single block of cover image. Here, we enhance the embedding capacity through weight matrix based data hiding scheme, where we can hide thirty six secret data bits within each block of cover image using dual image. As a result, In a (256×256) cover image, we can hide more than 2,60,100 bits. So, the payload is 1.98 bpp.
- To achieve reversibility in weighted matrix, we use dual image where stego pixel and original pixel are distribute among dual image and we can find the original pixel depending on the shared secret key bit stream ξ.

The rest of the paper is organized as follows. Section 2 describes literature review. Proposed data hiding scheme are discussed in Section 3. Experimental results with comparisons are discussed in Section 4. The steganographic security analysis are given in Section 5 and steganographic attacks are presented in Section 6. Finally, conclusions are given in Section 7.

2 Literature Review

The modern secret writings are tweaked the cover work in such a way that a secret message can be encoded within them. The secret message insertion may change every bit of information in the cover data. There are a number of ways to conceal information within the cover work. The most usual methodologies are based on the least significant bits (LSBs) substitution [2, 4, 25] and the modulus operation [3, 22, 26]. Reversible data hiding using block is commonly used to increase visual quality or to achieve reversibility [13, 14, 17, 19, 28]. Reversible data hiding (RDH) presented by Ni et al. [18] is based on histogram shifting with zero or minimum change of the pixel gray values. Multilevel reversible data hiding based on histogram shifting is proposed by Lin et al. [15] and Tsai et al. [24]. Adaptive reversible data hiding method using integer transform is presented by Peng et al. [20]. Designing a novel data hiding system accomplishing good visual quality, high embedding capacity, robustness and steganorgaphic protection is a technically challenging problem. Chang et al. [5] proposed a reversible data hiding scheme using two steganographic images. Lee et al. [12] developed a reversible data hiding scheme using dual stego-images, in which only one pixel value needs to be modified by at most plus or minus 1 for carrying two-bit data. Lee and Huang [11] developed a dual-image based reversible data hiding method that overcomes the drawbacks of the above methods. A secure data hiding scheme for binary images using a key matrix and a weight matrix W has been proposed by Tseng et al. [23] which can hide only 2 bits in a (3×3) block of pixels. Li Fan et al. [7] proposed an improved efficient data hiding scheme using weight matrix for gray scale images which can hide 4 bits in a (3×3) block. In both the matrix based schemes, only one modular sum of entry wise multiplication of weighted matrix W is performed with a (3×3) block of pixel in the original image. Only one embedding operation is performed with a single block and only 4 bits data embed within the block. High-capacity is still one of important research issues in data hiding. After the confidential message is extracted, the requirement for the image reversibility for the entire recovery of the original object without any distortion goes high. Here, we propose a high capacity reversible data hiding scheme using dual image, where we can hide thirty six bits secret data in each block. The scheme achieves good PSNR and high payload.

3 Proposed Scheme

Consider the weighted matrix W of size (3×3). Then we perform modular sum of entry wise multiplication of original image block $B_{3\times3}$ with weighted matrix W. We calculate data embedding position by subtracting the modular sum value v from secret data unit $D = d_1, d_2, \ldots$, that is, $p = d_i - v$. We check the sign of calculated position value (p). If the sign of p is positive/negative, then we increase/decrease the desired pixel value by one unit at the desired position of $B_{(3\times3)}$ pixel block. At the same time, we store the embedding position that is p by adding/subtracting within dual image stego major (SM) and stego auxiliary (SA). We distribute original pixel (OP) in one image and create a new pixel (NP). We then store NP in another image. Each time one OP is increased or decreased by p to generate the NP. Increase (or decrease) operation says the d value either 1 (or -1). SM or SA holds OP or NP decided by $\xi_{(\mod (j,length(\xi)))+1}$. Since ξ is the key in binary form, $\mod(j, length(\xi)) + 1$ indicates the index value where j=1, 2, 3, ... If $\xi_{(\mod (j,length(\xi)))+1} = 1$ then OP is stored in SM and NP is stored in SA; otherwise, OP is stored in SA and NP is stored in SM. After the block I_i completely examined, W is modified by Equation (1)

$$W_{i+1} = (W_i \times \kappa - 1) \mod 9, \text{ where } \gcd(\kappa, 9) = 1 \quad (1)$$

When all data are examined, then process will be stopped and finally two stego images SM and SA are produced. ξ, W and κ play an important role for data embedding and extraction. ξ is used for shuffling two modified pixels among dual image. The corresponding algorithm is described in Algorithm 1. The numerical illustration are shown in Figure 1.

Algorithm 1 Data embedding

Input: Cover Image ($I_{m\times n}$), Weight matrix ($W_{3\times 3}$), Data D=$d_1, d_2, d_3, \ldots$, where $d_i = r$ bits each, Shared secret key ξ of 128 bits.
Output: Two stego image $SM_{m\times n}$ and $SA_{m\times n}$;

Initialize: Dcount=Kcount=1; sq=3; SM=I; SA=I;
for (s=1) to (m/sq) do
  for t=1 to (n/sq) do
    $B_{st}(3\times 3) \leftarrow I_{m\times n}$**;**
    for i=(sq*(s-1))+1 to (sq*s) do
      for j=(sq*(t-1))+1 to (sq*t) do
        $SUM = B_{st} \otimes W_{st}$**;**
        v = SUM (mod16)**; p=**(d_{Dcount} **-v);**
        if (p> 0) then
          if (p> 8) then
            p=(16-p); d=-1
            d=1;
          end if
          if (p<-8) then
            p=abs(16+p); d=1
            p=abs(p); d=-1
          end if
        end if
        $B_{st}(x,y) = B_{st}(x,y) + d$ **if** $W_r(x,y)$**=p, where x=1,2,3 and y=1,2,3;**
        OP=$I_{m\times n}(i,j)$**; NP=**$I_{m\times n}(i,j) + (p\times d)$**;**
        if $(\xi(Kcount) = 1)$ **then**
          $SM_{m\times n}(i,j)$**=OP;** $SA_{m\times n}(i,j)$**=NP;**
          $SM_{m\times n}(i,j)$**=NP;** $SA_{m\times n}(i,j)$**=OP;**
          Dcount=Dcount+1; Kcount=Kcount+1;
          if (Kcount>length(ξ**)) then**
            Kcount=1;
          end if
        end if
        if (Dcount>length(D)) then
          goto Line-37
        end if
      end for
    end for
    $W_{st+1} = ((W_{st}\times\kappa - 1) \bmod 9)$**, where** $\gcd(\kappa, 9) = 1$**;**
  end for
end for
Produce $SM_{m\times n}$ and $SA_{m\times n}$ stego image;

At the receiver end, data are extracted from stego image SM and SA using secret keys ξ, κ and weighted matrix (W). Using ξ, we first rearrange the original pixel (OP) and new pixel (NP) by selecting 3×3 pixel block and generate the original image matrix (I) and new image matrix (NM) respectively. We generate a matrix (P_MX) of same size of I and NM.

$$P\_MX_{m\times n} = (I_{m\times n} \; - \; NM_{m\times n}) \tag{2}$$

The equation 2 is a simple matrix subtraction between I and NM. Now, we select each 3×3 block from I_i for entry-wise-multiplication with W. Before multiplication I_i will be modified to I_i' by changing one pixel mentioned by $P\_MX_i(x,y)$ where $x = 1,2,3$ and $y = 1,2,3$. That means for value at $P\_MX_i(1,1)$, I_i will be modified to I_i'

by increasing or decreasing 1 to one pixel that depends on sign of the value of $P\_MX_i(1,1)$. After that sum of the entry-wise-multiplication will be calculated to get the r bits data over modulo 2^r. Similarly for $P\_MX_i(1,2)$, I'_i will be modified to $I"_i$ and find the next r bits data. In this way, after 9 modification of I_i using $P\_MX_i(3,3)$, we modify W, then select I_{i+1} for next iteration. The algorithm of extraction procedure is shown in Algorithm-2. The numerical illustration is shown in Figure 2.

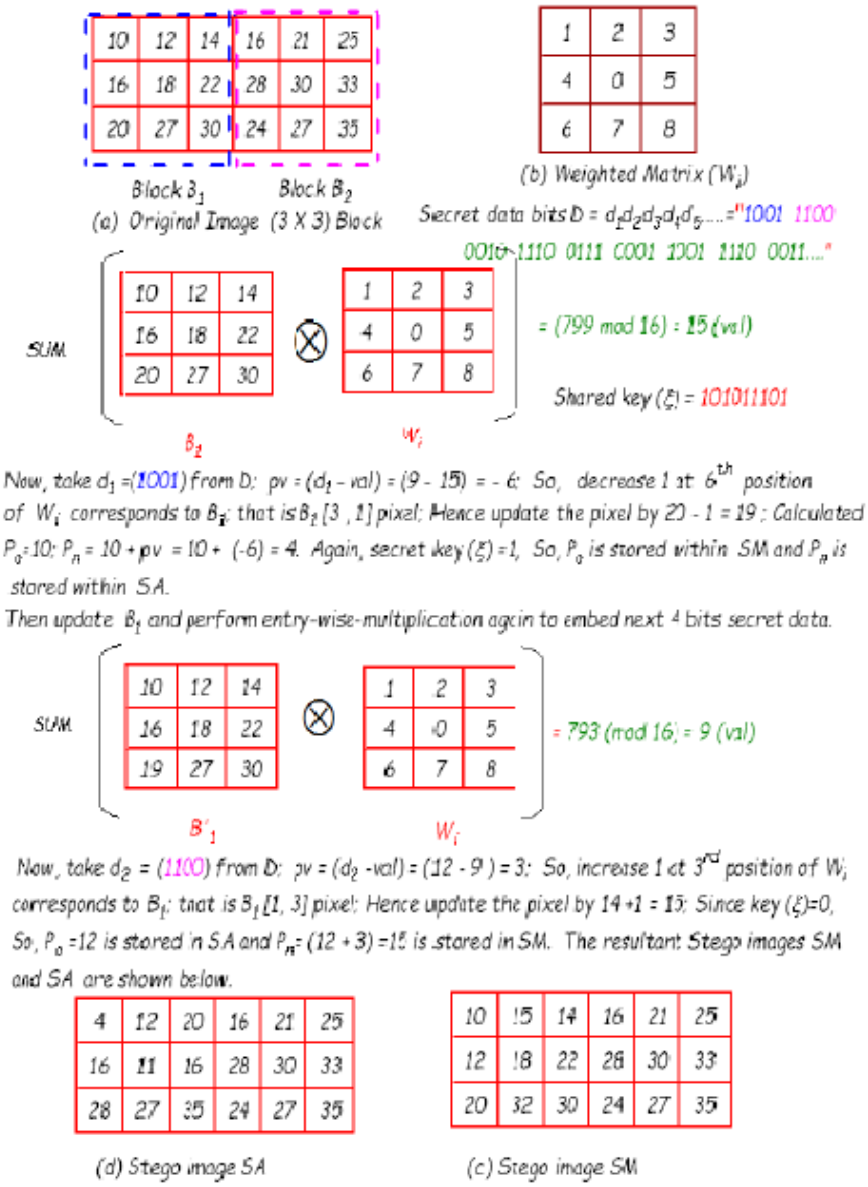

Figure 1: Example for data embedding

In this way hidden data D are extracted as well as original cover image is retrieved.

3.1 Overflow-Underflow Control

The p value is added or subtracted from OP to get NP and we put NP in one image and OP in other. So, OP is the original image and can not fall in overflow or underflow situation, but NP may fall. For example, if $OP = 248$ and $d = 1$, p value may be 8, then NP=(248+8)=256 which is greater then 255. So overflow situation will arise. Similarly, if OP=6 and $d = -1$ and p=7, then NP=(6-7)=-1 which is less then 0. So underflow situation will arise.

Algorithm 2 Data extraction

Input: Two stego image $SM_{m\times n}$ and $SA_{m\times n}$; Weight matrix($W_{3\times 3}$),shared secret key ξ of 128 bits; $Dlen$ is the data length;

Output: Cover Image ($I'_{m\times n}$), Data $D' = \{d'_1, d'_2, d'_3, \ldots,$ where $d'_i = 4$ bits each$\}$;

Initialize:$Dcount = Kcount = 1$; $sq = 3$; P_MX is a matrix that hold the p value; $I' = SM$;
for (s=1 to (m/sq)) **do**
  for (t=1 to (n/sq)) **do**
    for (i=(sq*(s-1))+1 to (sq*s)) **do**
      for (j=(sq*(t-1))+1 to (sq*t)) **do**
        if ($\xi(Kcount) = 1$) **then**
          $OP = SM_{m\times n}(i,j)$; $NP = SA_{m\times n}(i,j)$; $I'_{st}(i,j)$;
        else
          $OP = SA_{m\times n}(i,j)$; $NP = SM_{m\times n}(i,j)$; $I'_{st}(i,j)$;
        end if
        $P\_MX_{st}(i,j)$=$(NP - OP)$;
      end for
      $Kcount = Kcount + 1$;
      if ($Kcount > length(\xi)$) **then**
        $Kcount = 1$;
      end if
    end for
  end for
end for
for (s=1 to (m/sq)) **do**
  for (t=1 to (n/sq)) **do**
    $B_{st}(3\times 3) \leftarrow I'_{m\times n}$;
    for (i=(sq*(s-1))+1 to (sq*s)) **do**
      for (j=(sq*(t-1))+1 to (sq*t)) **do**
        if ($P\_MX_{st}(i,j)$ ¿ 0) **then**
          $p = P\_MX_{st}(i,j)$; d= 1;
        end if
        if ($P\_MX_{st}(i,j) \leq 0$) **then**
          $p = abs(P\_MX_{st}(i,j))$; d= -1;
        end if
        $B_{st}(x,y) = B_{st}(x,y) + \ d$ if $W_r(x,y)$=p, where x=1, 2, 3 and y=1, 2, 3;
        $SUM = B_{st} \otimes W_{st}$;
        (d'_{Dcount} = SUM (mod16); p=(d_{Dcount} -v);
        $Dcount = Dcount + 1$;
        if ($Dcount > Dlen$) **then**
          goto Line-43
        end if
      end for
    end for
    $W_{st+1} = ((W_{st} \times \kappa - 1) \bmod 9)$, where $\gcd(\kappa, 9) = 1$;
  end for
end for
Produce $I'_{m\times n}$ and $D' = \{d'_1, d'_2, d'_3, \ldots,$ where $d'_i = 4$ bits each

To overcome this problem, we use equation 3. If OP is greater then 247 or less then 8 then NP is calculated by

$$NP = \begin{cases} 247 + (p \times d), & \text{if } OP > 247 \\ 8 + (p \times d), & \text{if } OP < 8 \\ OP + (p \times d), & \text{otherwise.} \end{cases} \tag{3}$$

At the receiver end, receiver can easily found OP and NP by the key ξ. For extraction of p value we use Equation (4).

$$p = \begin{cases} NP - 247, & \text{if } OP > 247 \\ NP - 8, & \text{if } OP < 8 \\ NP - OP, & \text{otherwise.} \end{cases} \tag{4}$$

4 Experimental Results and Comparison

Our developed algorithms: data embedding and extraction are implemented in MATLAB Version 7.6.0.324 (R2008a). Here, the impairment is assessed by means of two factors namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio ($PSNR$) The MSE is calculated as by Equation (5)

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2}{(M \times N)}, \tag{5}$$

where M and N denote the total number of pixels in the horizontal and the vertical dimensions of the image respectively. $X(i,j)$ represents the pixels in the cover image and $Y(i,j)$ represents the pixels of the stego image.

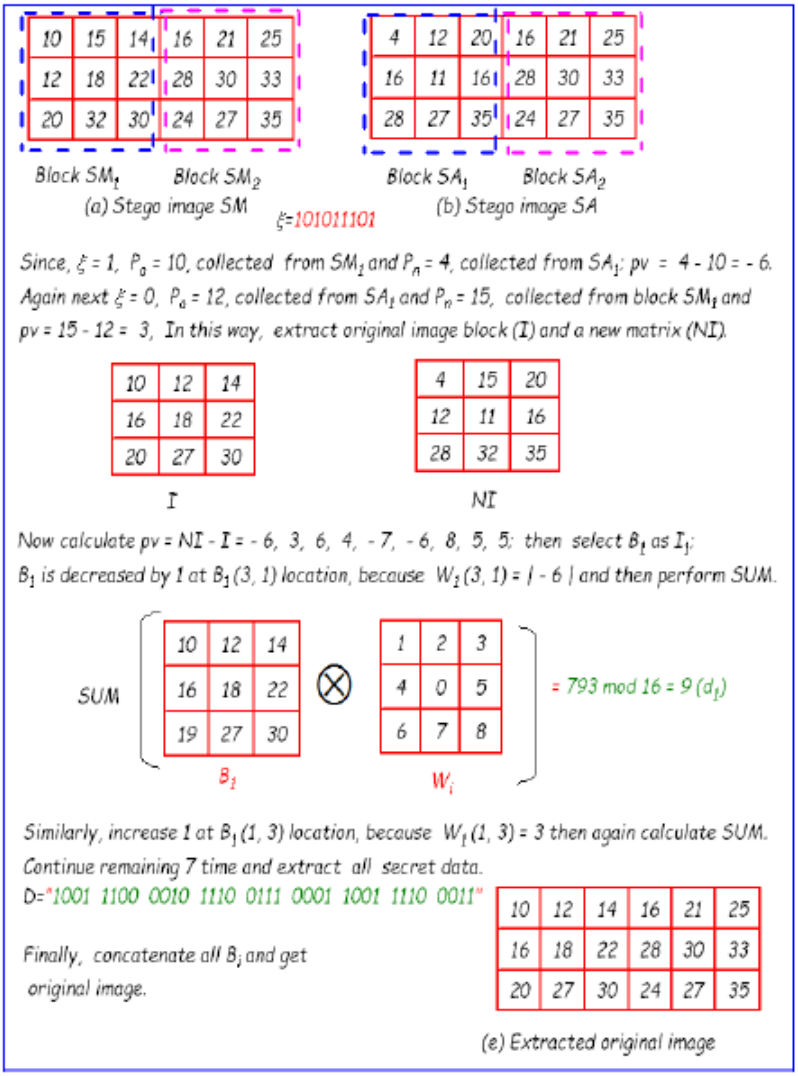

Figure 2: Extraction example

The difference between the original and stego images is assessed by the Peak Signal to Noise Ratio ($PSNR$). The analysis in terms of PSNR of cover image and stego image shows reasonably good results which is shown in Table 1.

Table 1: Data embedding capacity with PSNR

Image(I)	Data (Bits)	PSNR(SM)	PSNR(SA)
Camera Man	80,000	42.6752	43.1809
	1,60,000	39.7952	40.1716
	2,40,000	37.9778	38.4299
	2,60,096	37.6072	38.0798
House	80,000	42.6101	43.1188
	1,60,000	39.6894	40.1066
	2,40,000	37.9109	38.3755
	2,60,096	37.5586	38.0262
Jet Plane	80,000	42.6988	43.2139
	1,60,000	39.7976	40.1907
	2,40,000	37.9901	38.4492
	2,60,096	37.6146	38.0896
Lake	80,000	42.7090	43.1874
	1,60,000	39.7833	40.1606
	2,40,000	37.9790	38.4355
	2,60,096	37.6212	38.0835
Lena	80,000	42.7090	43.1928
	1,60,000	39.7856	40.1739
	2,40,000	37.9790	38.4502
	2,60,096	37.6379	38.0760
Little Lady	80,000	42.2023	42.6494
	1,60,000	39.5056	39.9096
	2,40,000	37.4163	37.8754
	2,60,096	36.9781	37.4429
Aerial	80,000	42.7000	43.2065
	1,60,000	39.7779	40.1823
	2,40,000	37.9767	38.4491
	2,60,096	37.6206	38.0687
Air Plane	80,000	42.5647	42.9980
	1,60,000	39.6874	40.0926
	2,40,000	37.9419	38.3705
	2,60,096	37.5712	38.0272
boat	80,000	42.6979	43.1925
	1,60,000	39.7214	40.1579
	2,40,000	37.9193	38.4441
	2,60,096	37.5853	38.0103
Clock	80,000	42.6866	43.1936
	1,60,000	39.7922	40.1734
	2,40,000	37.9918	38.4281
	2,60,096	37.6173	38.0780
Moon	80,000	42.6957	43.2003
	1,60,000	39.7922	40.1643
	2,40,000	37.9513	38.4238
	2,60,096	37.5963	38.0592
Baboon	80,000	42.6954	43.2206
	1,60,000	39.7351	40.1254
	2,40,000	37.9923	38.4215
	2,60,096	37.5951	38.0973
Gold-Hill	80,000	42.7115	43.2029
	1,60,000	39.7541	40.1211
	2,40,000	37.9523	38.4255
	2,60,096	37.5901	38.0843
Zelda	80,000	42.6758	43.1753
	1,60,000	39.7202	40.1463
	2,40,000	37.9443	38.4318
	2,60,096	37.5780	38.0073

PSNR is calculated using Equation (6).

$$PSNR = 10\ log_{10}\frac{255^2}{MSE}. \tag{6}$$

Higher the values of PSNR between two images, better the quality of the stego image and very similar to the cover image where as low PSNR demonstrates the opposite. The payload in terms of bits per pixel (bpp) is calculated by the following equation:

$$B = \frac{\frac{m}{x} \times \frac{n}{y} \times ((x \times y) \times r)}{(m \times n \times 2)}, \tag{7}$$

where m and n represent size of the input image, that is, $I_{(m \times n)}$). x and y represent size of the block. r represents the number of bits which are hidden in each block, 2 represents the number of stego images (dual). Consider $m = 256$, $n = 256$, $x = 3$, $y = 3$, $r = 4$ and $s = 2$. So, $B = 1.98$ bpp. The standard image are used for experiment. Figure 3 shows the input cover image and Figure 4 shows the dual stego image after embedding 2,60,096 bits.

Figure 3: Inputs images of size (256×256)

Table 2 presents a comparison between the proposed method and existing dual image based data hiding methods. We observed that the average PSNR of the stego images of the proposed method is around 37.7 dB when capacity is 2,60,096. The payload is 1.98 bpp. This capacity is higher than other existing techniques proposed by Lee et al.'s [11], Chang et al.'s [6], Qin et al.'s [21] and Lu et al.'s [16] So, in terms of payload our proposed method is superior, but the PSNR is slightly dropped.

5 Steganalysis

Steganalysis is the detection of secret data in stego images. Here, we describe and present the experimental results on J. Fridrich's RS steganalysis [9] and Cachin's KullbackLeibler (KL) divergence [1].

5.1 RS Steganalysis

We analyze our stego images by the J. Fridrich's RS steganalysis [9]. When the value of RS analysis is close to zero it means that the scheme is secure. It is observed from Table 3 and Table 4 that the values of R_M and R_{-M}, S_M and S_{-M} are nearly equal. Thus rule $R_M \cong R_{-M}$ and $S_M \cong S_{-M}$ are satisfied for the stego image in our scheme. So, the proposed method is secure against RS attack.

Table 2: Comparison between dual image based existing methods with our proposed method

Methods	PSNR	Images			
		Lena	Peppers	Boat	Goldhill
Chang et al.	SM	45.12	45.14	45.12	45.13
	SA	45.13	45.15	45.13	45.14
	Avg	45.13	45.15	45.13	45.14
	bpp	1	0.99	1	1
Chang et al.	SM	48.13	48.11	48.13	48.13
	SA	48.14	48.14	48.12	48.15
	Avg	48.14	48.13	48.13	48.14
	bpp	1	1	1	1
Lee et al.	SM	51.14	51.14	51.14	51.14
	SA	54.16	54.17	54.16	54.16
	Avg	52.65	52.66	52.65	52.65
	bpp	0.75	0.75	0.75	0.75
Lee et al.	SM	49.76	49.75	49.76	49.77
	SA	49.56	49.56	49.57	49.57
	Avg	49.66	49.66	49.67	49.67
	bpp	1.07	1.07	1.07	1.07
Chang et al.	SM	39.89	39.94	39.89	39.9
	SA	39.89	39.94	39.89	39.9
	Avg.	39.89	39.94	39.89	39.9
	bpp	1.53	1.52	1.53	1.53
Qin et al.	SM	52.11	51.25	51.11	52.11
	SA	41.34	41.52	41.57	41.34
	Avg.	46.72	46.39	46.84	46.72
	bpp	1.16	1.16	1.16	1.16
Lu et al.	SM	49.20	49.19	49.20	49.23
	SA	49.21	49.21	49.21	49.18
	Avg.	49.21	49.20	49.21	49.21
	bpp	1	0.99	1	1
Our Scheme	SM	37.63	37.61	37.58	37.59
	SA	38.07	38.06	38.01	38.08
	Avg.	37.85	37.83	37.79	37.83
	bpp	**1.98**	**1.98**	**1.98**	**1.98**

Table 3: RS analysis for Stego images SM of size 256×256)

Image	Data	SM				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	80000	6896	6922	3807	3817	0.0034
	160000	6403	6451	4270	4237	0.0076
	240000	6074	6138	4496	4468	0.0087
	260096	6152	6122	4527	4479	0.0073
Lena	80000	5490	5586	4142	4050	0.0195
	160000	5427	5550	4280	4149	0.0262
	240000	5422	5586	4424	4312	0.0280
	260096	5484	5535	4406	4448	0.0094
Baboon	80000	5872	5812	5010	5141	0.0176
	160000	5800	5815	5116	5112	0.0017
	240000	5851	5770	5118	5219	0.0166
	260096	5856	5757	5109	5215	0.0187

Figure 4: Stego image of size (256×256)

Table 4: RS analysis for stego images SA of size 256×256)

Image	Data	SA				
		R_M	R_{-M}	S_M	S_{-M}	RS value
Cameraman	80000	6961	6954	3788	3770	0.0023
	160000	6537	6422	4190	4248	0.0161
	240000	6179	6278	4426	4405	0.0113
	260096	6278	6244	4420	4447	0.0057
Lena	80000	5572	5483	4071	4100	0.0122
	160000	5476	5570	4308	4214	0.0192
	240000	5475	5452	4299	4354	0.0080
	260096	5409	5602	4495	4338	0.0353
Baboon	80000	5813	5831	5004	5091	0.0097
	160000	5841	5823	5077	5135	0.0070
	240000	5915	5701	5022	5251	0.0405
	260096	5803	5793	5088	5134	0.0051

5.2 Kullback-Leibler (K-L) Divergence

K-L divergence is also one of the popular security measures to analyze the data hiding schemes. It has been proposed by Cachin in 1998 [1]. Let p_m and q_n be probability measures for original image I and stego image S respectively. The KullbackLeibler (KL) divergence $D(S||I)$ (also known as Relative Entropy) is defined as Equation (8).

$$D(S||I) = \sum_{x \in G} q_n(x) log \frac{q_n(x)}{p_m(x)}, \tag{8}$$

where $x \in G = 0, 1, 2, \ldots, 255$ is the pixel value in gray scale images. We design our embedding algorithm such a manner that we get minimum value of K-L divergence which justifies the security. When K-L divergence between two probability distribution functions is zero then the system is perfectly secure. D$(S||I)$ is a nonnegative continuous function and equals to zero if and only if p_m and q_n coincide. Thus D$(S||I)$ can be naturally viewed as a distance between the measures p_m and q_n. In our experiment, it is shown that when the number of characters in the secret message increases, the K-L values in stego image is also increases. The K-L values in our experiment varies between 0.01 to 0.14 which is very less and implies that the proposed scheme provides secure hidden communication. K-L divergence values of cover image are shown in Table 5 and Table 6 shows the K-L values for SM and SA.

Table 5: Relative entropy of original image (256×256)

Cover Image	K-L
Cameraman	7.0299
Lena	7.4429
Baboon	7.2371

Table 6: Relative entropy of stego images SM and SA

Image	Data	SM		SA	
		K-L	Diff.	K-L	Diff.
Cameraman	80000	7.0572	0.04	7.1143	0.02
	160000	7.1220	0.01	7.1143	0.03
	240000	7.1547	0.14	7.1458	0.18
	260096	7.1555	0.14	7.1452	0.12
Lena	80000	7.4491	0.02	7.4494	0.01
	160000	7.4550	0.02	7.4562	0.01
	240000	7.4653	0.03	7.4622	0.03
	260096	7.4668	0.04	7.4654	0.03
Baboon	80000	7.2393	0.04	7.2394	0.04
	160000	7.2438	0.05	7.2437	0.05
	240000	7.2471	0.05	7.2461	0.05
	260096	7.2469	0.05	7.2475	0.05

6 Steganographic Attack

We analyze our propose scheme through various stego attacks include statistical attack, Jeremiah J. Harmsena's Histogram attack and brute force attack. We propose our data embedding algorithm which resist against all these types of attacks making eavesdropper unable to retain the hidden message.

6.1 Statistical Attack

In this section, we analyze the statistical attacks by finding Standard Deviation (SD) and Correlation Coefficient (CC) of cover and stego images of our proposed scheme. We calculate the (SD) and (CC) of cover and stego images that is before and after data embedding which are summarized in Table 7. Minimizing parameters difference is one

of the primary aims in order to get rid of statistical attacks. It is observed that there is no substantial divergence between the SD of the cover-image and the stego-images. This study shows that the magnitude of change in stego-images based on image parameters is small from a cover image. Since the image parameters have not changed much, the method offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates secure data hiding scheme.

Table 7: Standard deviation (SD) and correlation coefficient (CC) of proposed method

Image	SD			CC		
	I	SM	SA	I & SM	I & SA	SM & SA
Cameraman	61.58	61.70	61.67	0.99	0.99	0.99
Lena	47.83	47.96	47.94	0.99	0.99	0.99
Baboon	38.37	38.48	38.50	0.99	0.99	0.99

6.2 Histogram Attack

A new steganalytic attack has been proposed by Jeremiah J. Harmsena [10] in 2003. Harmsen based his attack on the fact that noise adding in the spatial domain corresponds to low-pass filtering of the histogram. Figure 5 describes the histogram of the cover and stego image and their difference histograms. The stego image is 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 Equation (9).

$$D_h = \sum_{m=1}^{255} |h_m^{'} - h_m| \tag{9}$$

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

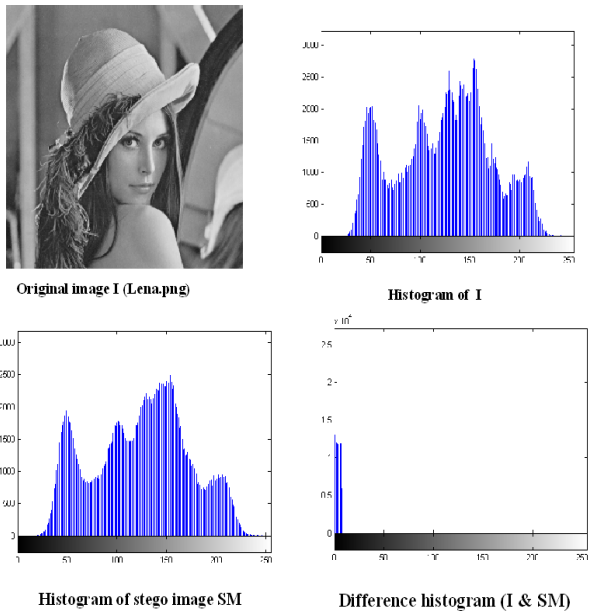

Figure 5: Histogram of original and stego image and their difference

6.3 Brute Force Attack

The proposed scheme produces dual stego images which protect secret information through weighted matrix. We embed the data embedding position (p), not the original information within dual stego images. We use κ to update

weighted matrix for each selected block. The scheme is secure to prevent possible malicious attacks. Figure 6 shows the example of getting noise data when applied wrong key and wrong weighted matrix are used to revel the hidden message. If the malicious attacker holds the original image and stego image and is fully aware of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct secret key and correct weighted matrix. Similarly, if the malicious attacker are fully aware about stego image and weighted matrix of the proposed scheme, the hidden message still cannot be correctly revealed without knowing the correct key ξ and κ. Furthermore, the attacker may employ the brute force attack that tries all possible permutation to reveal the hidden message. Maximum possibilities of weighted matrix to embed r bits data length in each block is $(2^{r-1}+1)!$. We have used $(M \times N)$ original matrix and partitioned (3×3) blocks. Total number of blocks are $\lfloor \frac{M}{3} \rfloor \times \lfloor \frac{N}{3} \rfloor$ and each block is used a modified weighted matrix. So, the number of trials to reveal the hidden message are $((2^{r-1}+1)!)^{\lfloor \frac{M}{3} \rfloor \times \lfloor \frac{N}{3} \rfloor}$. In our scheme, key ξ is used for pixel distribution among dual image. So, if key length is 128 bits then for (256×256) image with $r = 4$, number of trails will be $(2^{128} \times 3,62,880)^{7281}$ which is computationally infeasible for current computers by an adversary.

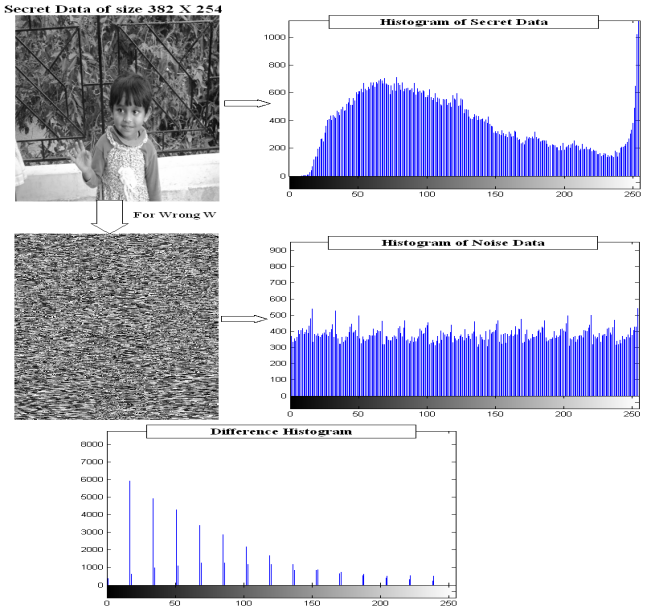

Figure 6: Noise like secret data for wrong weighted matrix

The proposed scheme has achieved stronger robustness against several attacks. Furthermore, the secret information can be retrieved without encountering any loss of data and recovered original image successfully from stego image.

7 Conclusion

A new reversible data hiding scheme through weighted matrix using dual image is proposed in this paper. We have modified weighted matrix for different blocks using κ to enhance security in data hiding. In this scheme, we have achieved PSNR greater than 39 dB and payload greater than 1.98 bpp. We have also tested our scheme using RS steganalysis, calculate Kullback-Leibler (K-L) divergence, statistical analysis (such as Standard Deviation and Correlation Coefficient) which have provide promising results. We have tested our scheme by several steganographic attacks such as histogram attack and brute force attack. We have observed that the scheme is secure and robust against all known attacks.

References

[1] C. Cachin, "An information-theoretic model for steganography," in *Lecture Notes in Computer Science*, vol. 1525, Springer-Verlag, pp. 306–318, 1998.

[2] C. Chan, L. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 474–496, 2004.

[3] C. Chang, C. Chan, Y. Fan, "Image hiding scheme with modulus function and dynamic programming," *Pattern Recognition*, vol. 39, no. 6, pp. 1155–1167, 2006.

[4] C. Chang, J. Hsiao, C. Chan, "Finding optimal least-significant-bits substitutionin image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1595, 2003.
[5] C. C. Chang, T. D. Kieu, and Y. C. Chou, "Reversible data hiding scheme using two steganographic images," in *Proceedings of IEEE Region 10 International Conference (TENCON'07)*, pp. 1–4, 2007.
[6] C. C. Chang, T. C. Lu, G. Horng, Y. H. Huang, and Y. M. Hsu, "A high payload data embedding scheme using dual stego-images with reversibility," in *Proceedings of Third International Conference on Information, Communications and Signal Processing*, pp. 1–5, 2013.
[7] L. Fan, T. Gao, Y. Cao, "Improving the embedding efficiency of weight matrix-based steganography for grayscale images," *Computers and Electrical Engineering*, vol. 39, pp. 873–881, 2013.
[8] L. Fan, T. Gao, Q. Yang, Y. Cao, "An extended matrix encoding algorithm for steganography of high embedding efficiency," *Computers & Electrical Engineering*, vol. 37, pp. 973–981, 2011.
[9] J. Fridrich, J. Goljan, R. Du, "Invertible authentication," in *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents*, vol.4314, SanJose, CA, pp. 197–208, Jan. 2001.
[10] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proceedings of SPIE Electronic Imaging*, Santa Clara, Jan. 21–24, 2003.
[11] C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," *Telecommunication Systems*, vol. 52, No. 4, pp. 2237–2247, 2013.
[12] C. F. Lee, K. H. Wang, C. C. Chang, and 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] P. S. Liao, J. S. Pan, Y. H. Chen, B. Y. Liao, "A lossless watermarking technique for halftone images," in *Proceedings of KES 2005*, LNCS 3682, Springer, pp. 593–599, 2005.
[14] B. K. Lien, Y. Lin, "High-capacity reversible data hiding by maximum-span pairing," *Multimedia Tools and Applications*, vol. 52, pp. 499–511, 2011.
[15] C. C. Lin, W. L. Tai, C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 35, pp. 82–91, 2008.
[16] 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.
[17] Z. M. Lu, H. Luo, J. S. Pan, "Reversible watermarking for error diffused halftone image using statistical features," in *Proceedings of IWDW 2006*, LNCS 4283, Springer, pp. 71–81, 2006.
[18] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.
[19] J. S. Pan, H. Luo, Z. M. Lu, "A lossless watermarking scheme for halftone image authentication," *International Journal of Computer Science and Network Security*, vol. 6, no. 2b, pp. 147–151, 2006.
[20] F. Peng, X. Li, B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Process.* vol. 92, pp. 54–62, 2012.
[21] 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.
[22] C. Thien, J. Lin, "A simple and high-hiding capacity method for hiding digitby-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875–2881, 2003.
[23] Y. C. Tseng, Y. Y. Chen, H. K. Pan, "A secure data hiding scheme for binary images," *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1227–1231, 2002.
[24] P. Y. Tsai, Y. C. Hu, H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Processing*, vol. 89, no. 11, pp. 29–43, 2009.
[25] R. Wang, C. Lin, J. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.
[26] S. J. Wang, "Steganography of capacity required using modulo operator forembedding secret image," *Applied Mathematics and Computation*, vol. 164, no. 1, pp. 99–116, 2005.
[27] A. Westfeld, "F5 - A steganographic algorithm: High capacity despite better steganalysis," *Lect Notes on Computer Science*, vol. 2137, pp. 289–302, 2001.
[28] F. X. Yu, H. Luo, S. C. Chu, "Lossless data hiding for halftone images," in *Information Hiding and Applications*, Springer, vol. 227, pp. 181–203, 2009.

Biography

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. He has recently submitted his Ph.D. Thesis

on Design and Implementation of Dual Image based Reversible Data Hiding Techniques. His research interest includes Image Processing, Data Hiding and Steganography. He has published more than 30 papers in National and International Journal and Conferences.