A Novel Approach on Reversible Data Hiding Using Bit-Reversal Permutation

[1]KankanaDatta [2]Manasi Jana

[1,2]Department of Computer Applications Haldia Institute of Technology India

Abstract

Reversible data hiding method is a new concept for data hiding and information security. Being reversible, both the original data and the embedded data can be completely restored. In this paper, we have proposed a novel approach of reversible data hiding scheme using bit reversal permutation. Here the secret data is embedded in the cover image by XOR operation followed by bit reversal permutation.At the receiver end, we have extracted the secret message successfully and recover original cover image from stego image without any distortion. We also compared our proposed scheme with other state-of-the-art schemes to show the efficiency of the proposed scheme. The experimental results show that this methodology can achieve very high embedding capacity and keep the distortion low.

Keywords:

Reversible data hiding, Bit reversal permutation, XOR

1 Introduction

Nowadays, people are communicating each other through Internet and sharing their multimedia data through Internet especially in this Covid situation. So, it is necessary to protect the documents from intruder. Steganography or data hiding [1,2] and digital watermarking [3] are two ways to accomplish this goal. Various data hiding techniques have been proposed in different literatures [4,5]. Data hiding or steganography may be implemented on both domain such as spatial domain [6] and transform domain [7]. In special domain, the secret data are embedded into the pixel of cover media whereas in frequency domain, the secret data is embedded after transforming the cover image into frequency coefficients. Reversible data hiding [8] is one of the most interesting topics among researchers. For some applications, such as medical images, remote sensing images, military maps, reversible data hiding is the best solution to restore original images. In this paper, we have proposed a novel approach of reversible data hiding technique using bit-reversal permutation which provides a high embedding capacity and low image distortion. The contribution of the proposed scheme is illustrated below.

(i) **Reversibility:** A novel reversible data hiding technique has been proposed using bit reversal permutation.

(ii) **Imperceptibility:** Here, secret data is embedded at LSB (Least Significant Bit) of each pixel. The proposed scheme produces high imperceptibility as only one bit of each pixel of cover image has been changed.

(iii) **High embedding capacity:** In each pixel of cover image, one bit of secret message is embedded which results in high embedding capacity.

After introduction, the remaining paper has been arranged as follows. Section 2 describes the related works while section 3 introduces the encryption and decryption algorithm of proposed scheme with numerical example. Section 4 analyses the experimental results and comparisons. Finally, conclusion has been presented at section 5.

2. Related works

Most of the reversible data-hiding techniques are designed using Difference Expansion (DE) [9], Interpolation [10] and Histogram modification [11]. Tian [9] proposed a reversible data hiding technique with 0.5 bpp embedding capacity. In 2006, Ni et. al[12] proposed a reversible technique based on histogram shifting. It achieves a stego image with good quality but having low embedding capacity due to its peak height. Image interpolation [13 ,14] is a new concept to implement reversal data hiding where interpolated values are computed from the pivot pixels and data are embedded into the interpolated pixels. Here we have designed a novel concept of reversible data hiding technique based on bit-reversal permutation [15].

3. Proposed Scheme

This section describes the proposed scheme elaborately. The proposed scheme combines the bit-reversal permutation technique with data embedding method in LSB. The technique of bit-reversal permutation is illustrated as follows.

3.1 Bit –reversal permutation

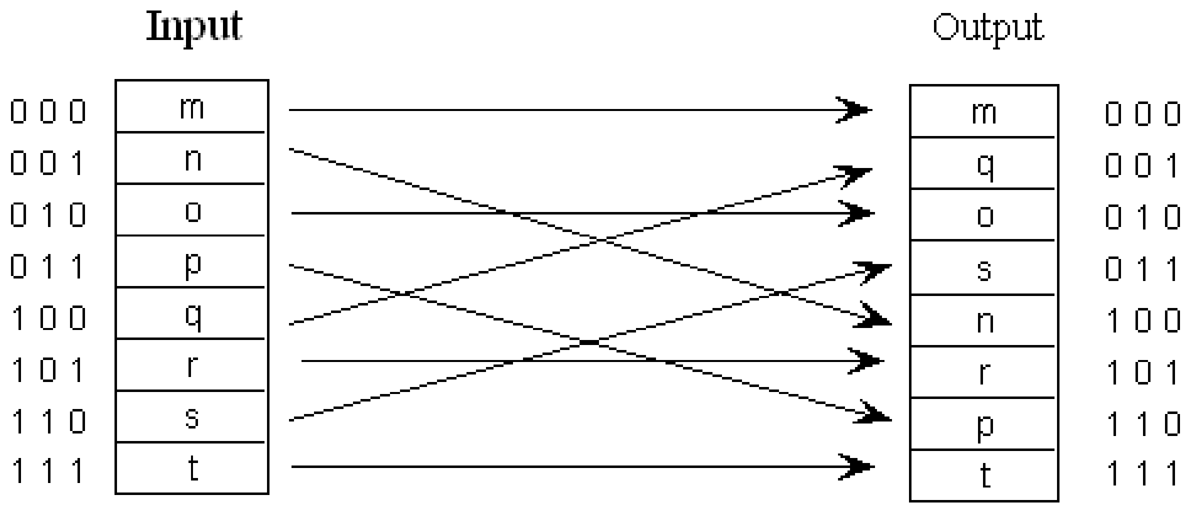


Fig 1 Example of Bit Reversal Permutation

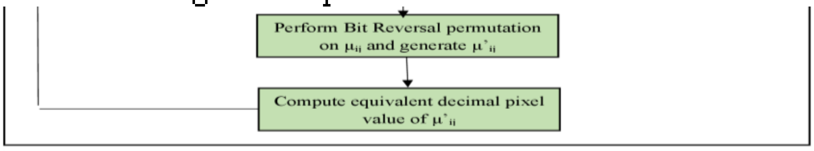

Perform Bit Reversal permutation on μ_{ij} and generate μ'_{ij}
Compute equivalent decimal pixel value of μ'_{ij}

Fig: 2 Block Diagram of data Encryption of the proposed scheme

Bit-reversal permutation is a permutation of a set of n items, where n=2^k. It is defined by indexing the elements from 0 to n-1 and then each item is mapped to a new position which is the reverse value of binary representation of each index number.Consider the sequence of eight letters m ,n, o, p, q, r, s, t. Their indexes in binary representation are 000, 001, 010, 011, 100, 101, 110 and 111. After reversal these become 000, 100, 010, 110, 001, 101, 011 and 111. Thus letter m is mapped to position (000), letter n is mapped to position 100(5th position) etc. as shown in Fig 1.

Using Bit-reversal permutation, we have proposed a reversible data hiding technique which enhances the payload capacity of cover image I and make our scheme reversible. It means by decryption algorithm receiver can retrieve the secret message along with cover image I from the stego image I' without any distortion. Our Proposed scheme is the combination of two parts - encryption and decryption.

3.2 Encryption Design

In the proposed scheme initially the 512 X 512 grayscale cover image I is divided into d × d non-overlapping equal blocks which are called bitmaps, denoted by B_i where irepresents the position of bitmap where it is appearing in I. The proposed encryption algorithm is applied on each B_i individually where each bitmap B_i holds the d X d number of pixels. The block diagram of the total encryption procedure of the proposed scheme is shown in Fig 2.

In the proposed scheme, at first a pixel P_{ij}(where irepresents the position of bitmap B_i where it is appearing in I and j represents the position of the pixel in bitmap B_i) is selected from a particular B_i and converted it into 8-bits binary form. In the next step, an XOR operation is performed on 8-bit binary representation of pixel $P_{ij}$and the secret message bit S_j (where j represents the position of secret bit S) and produces a 8-bit binary number which is denoted by μ_{ij}. There after a comparison is made between LSB of $\mu_{ij}$and secret bit S_j. If both are equal then put zero ('0') within a reference table γ_j(where j represents the location of the reference table), otherwise put one

(‘1’) within a reference table γ_j(where j represents the location of the reference table). After that the Bit-Reversal Permutation technique is applied on $\mu_{ij}$and generates a 8-bit binary number which is represented by μ'_{ij}. At last the equivalent decimal value of μ'_{ij} is calculated and this value is considered as a new pixel value for the stego image I’. This procedure is applied on all the pixels of a B_i. The above encryption technique iscontinued until or unless all the bitmaps of cover image I are covered.

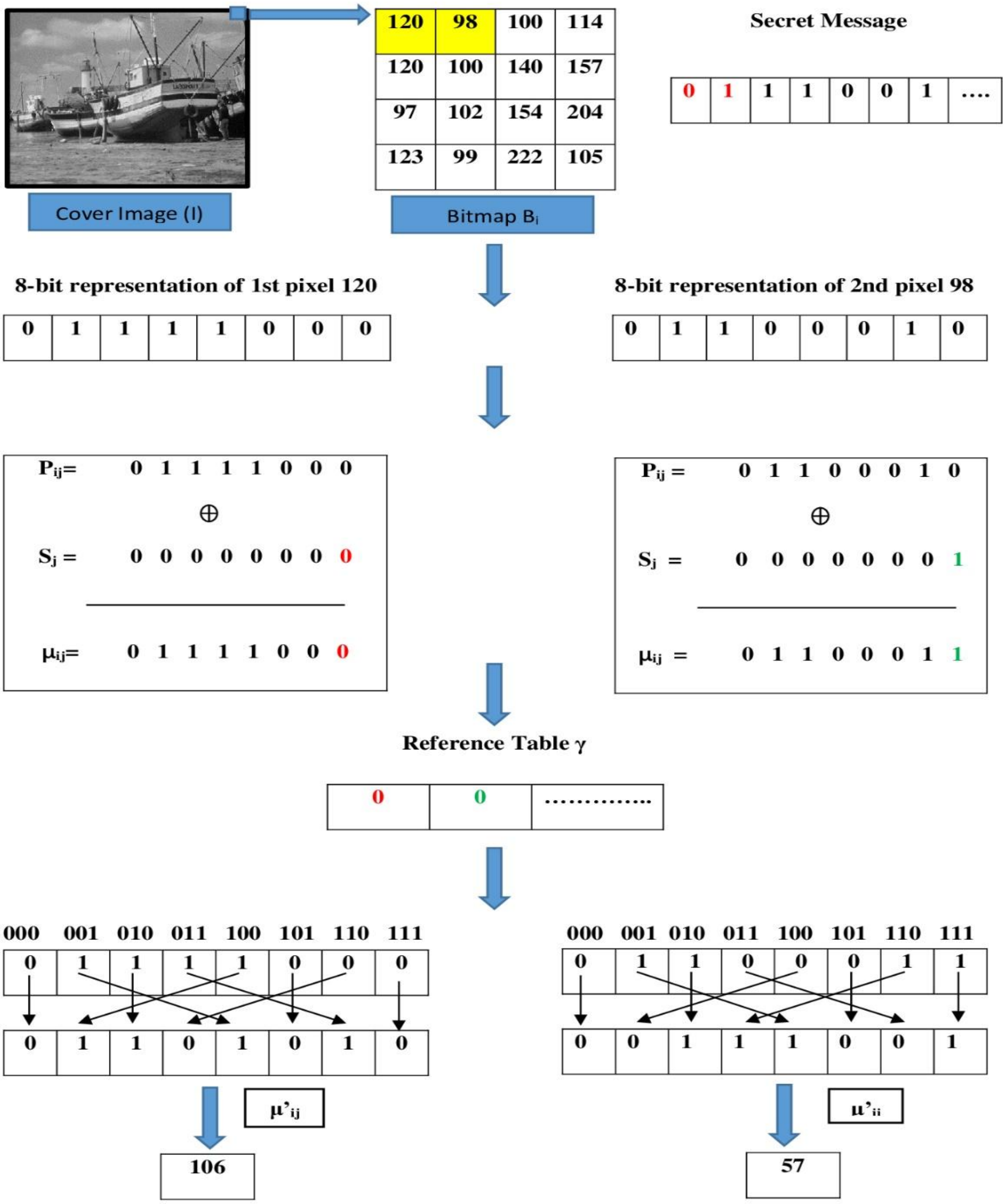


Fig:3 Data Encryption design for two pixels

The step by step encryption technique for a bitmap B_i is depicted by the algorithm 1.

Input:A 4 × 4 bitmap B_i (irepresents the position of bitmap B_i where it is appearing in I),
Secret Message S.

The following algorithm is applicable for each bitmap B_i separately and these steps are repeated for all bitmaps until or unless all secret bits are embedded successfully.

Output: Stego Image I'.

```
Begin
Step 1: For j=1 to 16
Step 2: Select a pixel $P_{ij}$ and find it into 8-bit binary number.
Step 3:Select Message bit $S_j$.
Step 4:Set $\mu_{ij} = P_{ij} \oplus S_j$
Step 5.i:If LSBof$\mu_{ij}$ = $S_j$ Then
            Put 0 into the $\gamma_j$.
ii. Else
            Put 1 into the$\gamma_j$.
    End if
Step 6: Perform Bit Reversal permutation on $\mu_{ij}$ and generate $\mu'_{ij}$.
Step 7: Find the equivalent decimal pixel value of $\mu'_{ij}$.
Step 8: Finally combine all the bitmaps $B_i$ and generate stego image I'.
Step 9:End.
```

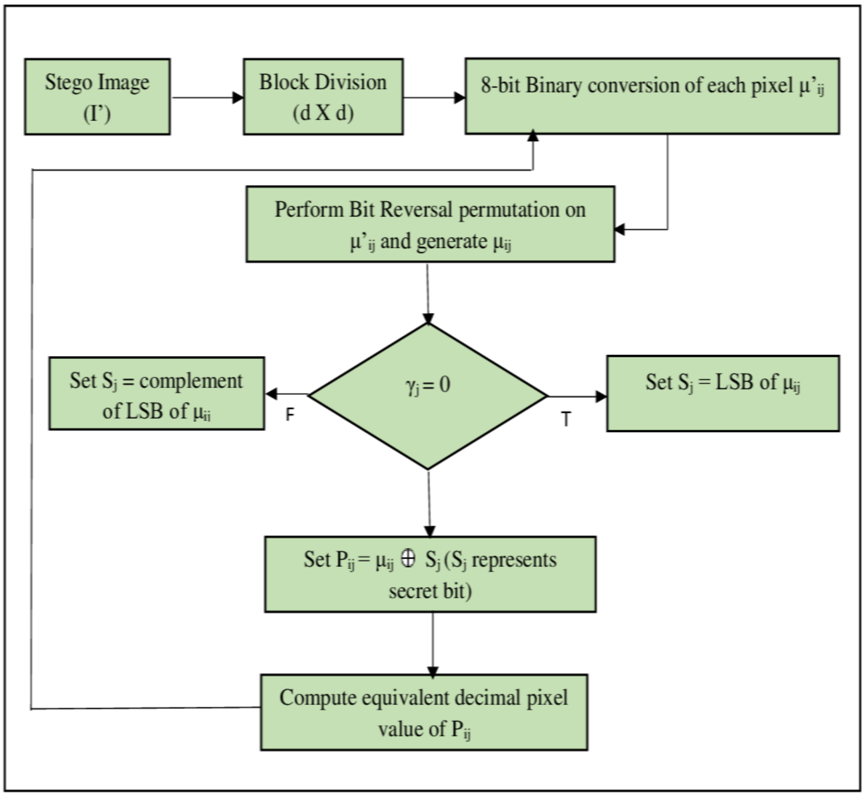

Stego Image (I')
Block Division (d X d)
8-bit Binary conversion of each pixel μ'ij
Perform Bit Reversal permutation on μ'ij and generate μij
Set Sj = complement of LSB of μii
F
γj = 0
T
Set Sj = LSB of μij
Set Pij = μij ⊕ Sj (Sj represents secret bit)
Compute equivalent decimal pixel value of Pij

Fig: 4 Block Diagram of data Decryption of the proposed scheme

Algorithm 1 Encryption algorithm for bitmap B_i

3.2 Numerical Example for Encryption technique:

The numerical example of the proposed encryption algorithm is shown in Fig 3. In this example, for a 4 X 4 bitmap B_i, the 8-bit binary representation of two pixels 'P_{ij}=120' and 'P_{ij}=98' are '01111000' and '01100010' respectively. Here two secret bits '$\mathbf{S_j}$ =0' and '$\mathbf{S_j}$ =1' are embedded into '01111000' and '01100010' respectively by XOR operation which produces 'μ_{ij}= 01111000' and 'μ_{ij}= 01111000' respectively as output. For both the cases as the LSB of μ_{ij} is equal to the secret bit S_j (in the first case both are 0 and in the second case both are 1), so a zero (0) is assign in the j^{th}position of the reference table γ individually. After that Bit Reversal permutation technique is applied on 'μ_{ij}= 01111000' and 'μ_{ij}= 01111000' separately and generated 'μ'_{ij}= 01101010' and 'μ'_{ij}= 00111001' respectively. Finally two new pixels are produced for stego image I' by converting μ'_{ij} in decimal. According to this example the two new pixel values are '106' and '57' respectively. This process will be applicable for all the pixels of all the bitmaps of the cover image I. At the end of this technique all bitmaps are combined together and produced a stego image I' which will be sent to the receiver along with the reference table γ for decryption the secret message.

3.3 Decryption Design

Since the proposed scheme provides the reversible data hiding concept, so here receiver retrieves the secret message along with the original cover image I without any distortion. In the decryption stage, initially the 512 X 512 grayscale stego image I' is separated into d × d non-overlapping equal blocks which are called bitmaps, denoted by B'_i where irepresents the position of bitmap where it is appearing in I'. The decryption algorithm is applied on each B'_iindividually where each bitmap B'_i holds the d x d number of pixels. The block diagram of the total decryption procedure of the proposed scheme is depicted in Fig 4.

In this proposed scheme, at first a pixel μ'_{ij}(where irepresents the position of bitmap B'_i where it is appearing in I' and j represents the position of the pixel in bitmap B'_i) is chosen from a particular B'_i and converted it into 8-bit binary numbers. In the next step, $\mu_{ij}$is generated by performing the Bit-Reversal Permutation technique on μ'_{ij}. After that if the value of the reference table γ_j(where j represents the location of the reference table) is equal to '0' then the retrieved message bit (S_j) is LSB of μ_{ij} and if the value of the reference table γ_j(where j represents the location of the reference table) is equal to '1' then the retrievedmessage bit (S_j) is complement of LSB of μ_{ij}. After extracting the message bit an XOR operation is performed on μ_{ij} and the secret message bit S_j (where j represents the position of secret bit S) and generated an 8-bit binary number denoted by P_{ij}. At last the equivalent decimal value of P_{ij} is computed and this value is considered as an original pixel value of the cover image I. This procedure is applied on all the pixels of a B'_i. The above decryption technique is continued until or unless all the bitmaps of stego image I' are covered.

The step by step decryption technique for a bitmap B'_i is depicted by the algorithm 2.

Input:A 4 × 4 bitmap B'_i(irepresents the position of bitmap B'_i where it is appearing in I'),
Reference Table γ.

The following algorithm is applicable for each bitmap B_i individually and these steps are repeated for all bitmaps until or unless all secret bits are extracted successfully.

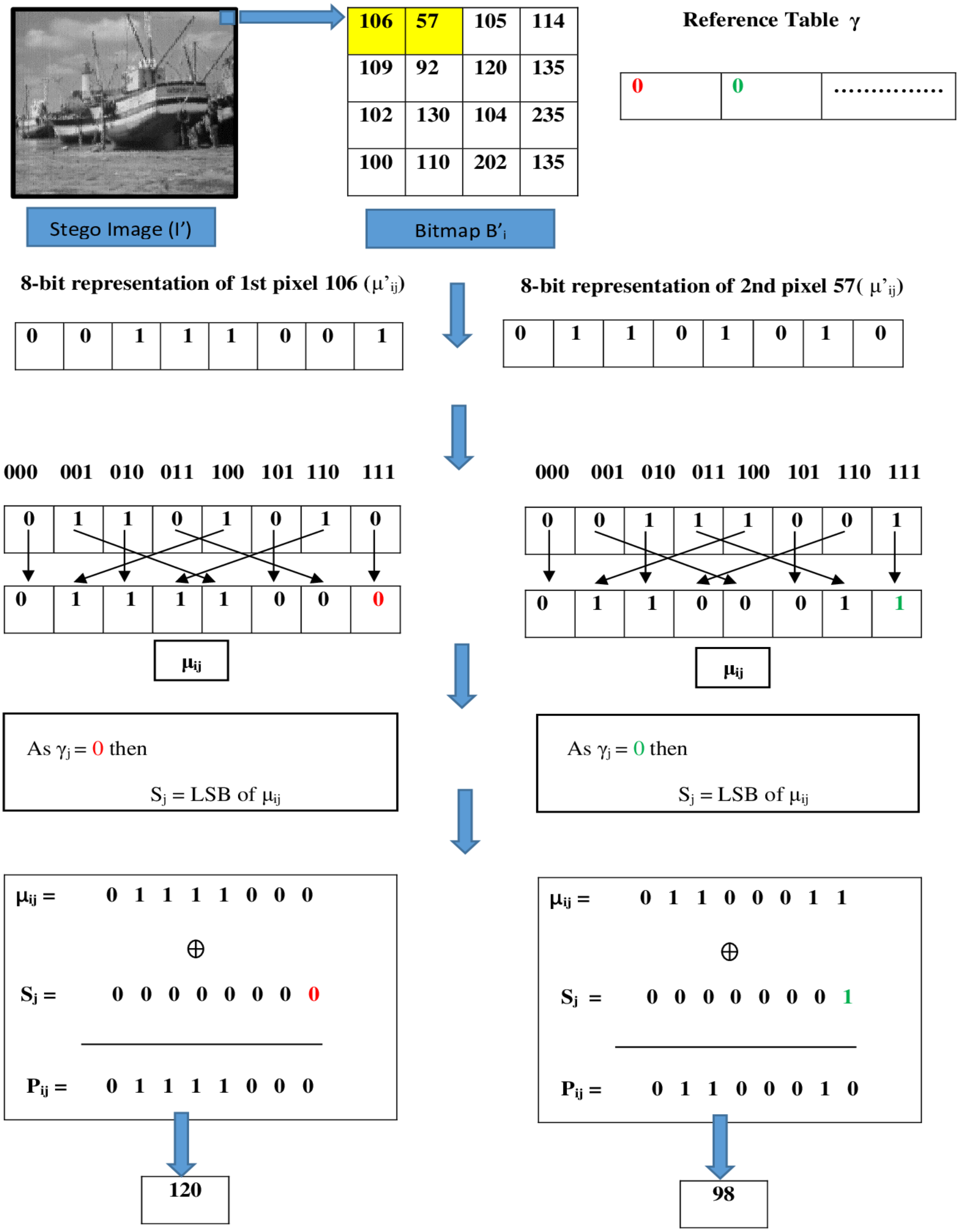
```
Output:Cover Image I, Secret Message S.
Begin
Step 1: For j=1 to 16
Step 2: Select a pixel $\mu'_{ij}$ and convert it into 8-bit binary number.
Step 3:Perform Bit Reversal permutation on $\mu'_{ij}$ and generate$\mu_{ij}$.
Step 4.i.If$\gamma_j$= 0 then
                Set $S_j$ = LSB of$\mu_{ij}$.
ii. Else
                Set$S_j$ = complement of LSB of$\mu_{ij}$
        End if
Step 5:Set $P_{ij}$= $\mu_{ij} \oplus S_j$
```

Step 6: Find the equivalent decimal pixel value of P_{ij}.

Step 7: Finally combine all the bitmaps B_i and generate cover image I.

Step 8: End.

Algorithm 2 Decryption algorithm for bitmap B’$_i$



106	57	105	114
109	92	120	135
102	130	104	235
100	110	202	135

Fig:5 Data Decryption design for two pixels

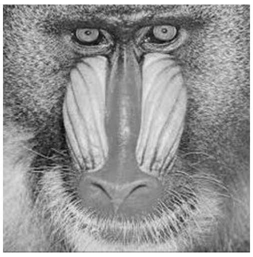
3.4 Numerical Example for Decryption technique:

The numerical example of the proposed decryption algorithm is shown in Fig 5. In this example, for a 4 X 4 bitmap B'_j, the 8-bit binary representation of two pixels ‘μ'_{ij}=106’ and ‘μ'_{ij}=57’ are ‘00111001’ and ‘01101010’ respectively. After that Bit Reversal permutation technique is applied on ‘μ'_{ij}= 00111001’ and ‘μ'_{ij}= 01101010’ individually and generated ‘μ_{ij}= 01111000’ and ‘μ_{ij}= 01100011’ respectively. Science the value of received reference table is ‘γ_j=0’ for both the cases so the LSB of μ_{ij} is extracted as a secret message bit. In this example, secret bits ‘S_j=0’ and ‘S_j =1’ are retrieved from the first and second case respectively. To retrieve the original pixel value ‘P_{ij}=01111000’and‘P_{ij}=01100010’, an XOR operation is performed on $\mu_{ij}$and S_j. Finally two original pixels ‘120’ and ‘98’ are retrieved by converting ‘P_{ij}=01111000’and‘P_{ij}=01100010’in decimal. This process will be applicable for all the pixels of all the bitmaps of the stego image I’. At the end of this technique all bitmaps are combined together to get the original cover image I.

4 Experimental Results and comparisons:

The proposed scheme has been implemented using MATLAB R2016a platform. We have used different type of images such as six gray scale USC-SIPI images (512x512) and UCID images (512x512) for experimental results as shown in Fig 6. We also have used some logo gray scale images (80 x 80) as secret images as shown in Fig 7. The proposed scheme may also be used as authentication purposes due to using of logo images as secret message. The stego images (512 x 512) as shown in Fig. 8 are generated after encrypting the secret image using bit reversal permutation and XOR operation.

We have evaluated the proposed scheme in terms of PSNR, SSIM, Q-index and payload as shown in Table 1. It is clear from the table that the range of PSNR value of stego image is 34.18 to 35.98 which shows good imperceptibility of the proposed scheme. The average value of SSIM and Q-index of proposed scheme is 0.92 and 0.94 respectively which shows satisfactorily similarity between cover image and stego image of the proposed scheme.

USC-SIPI images	 (a)	 (b)	 (c)
	 (d)	 (e)	 (f)
	 (g)	 (h)	 (i)

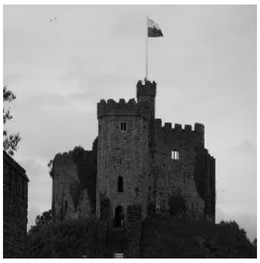
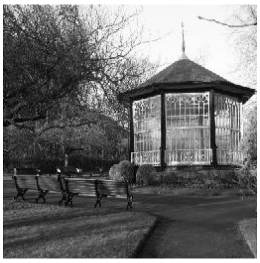
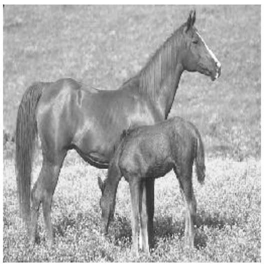
UCID images	 **(j)**	 **(k)**	 **(l)**

Fig. 6Test images (512x512) of the proposed scheme (a) Lena (b) Baboon (c) Pepper (d) Lake (e) Tiffany (f) Boat (g) UCID 1 (h) UCID 2 (i) UCID 3 (j) UCID 4 (k) UCID 5 (l) UCID 6

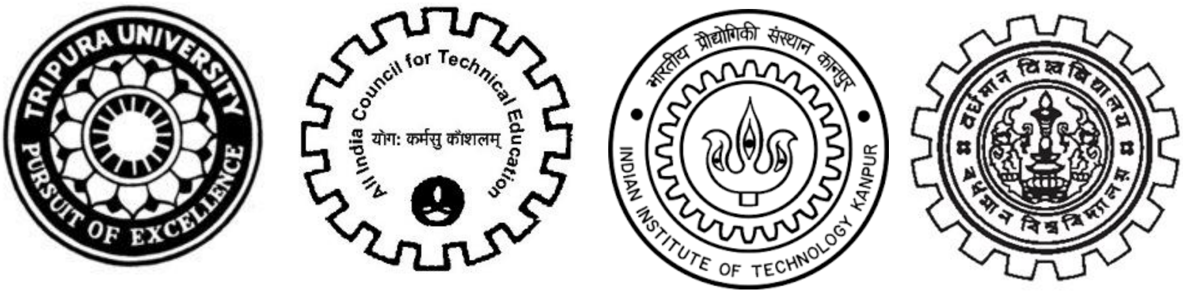
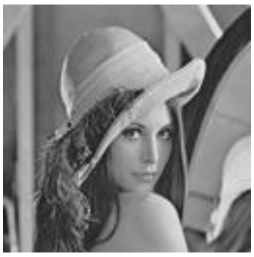
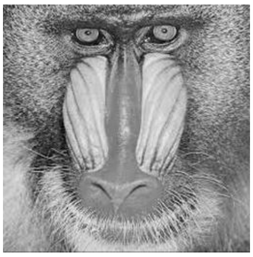

TRIPURA UNIVERSITY
PURSUIT OF EXCELLENCE
All India Council for Technical Education
योग: कर्मसु कौशलम्
भारतीय प्रौद्योगिकी संस्थान कानपुर
INDIAN INSTITUTE OF TECHNOLOGY KANPUR

Fig. 7 Secret images (80 x 80) used in proposed scheme

USC-SIPI images	 **(a)**	 **(b)**	**(c)**
	(d)	**(e)**	**(f)**

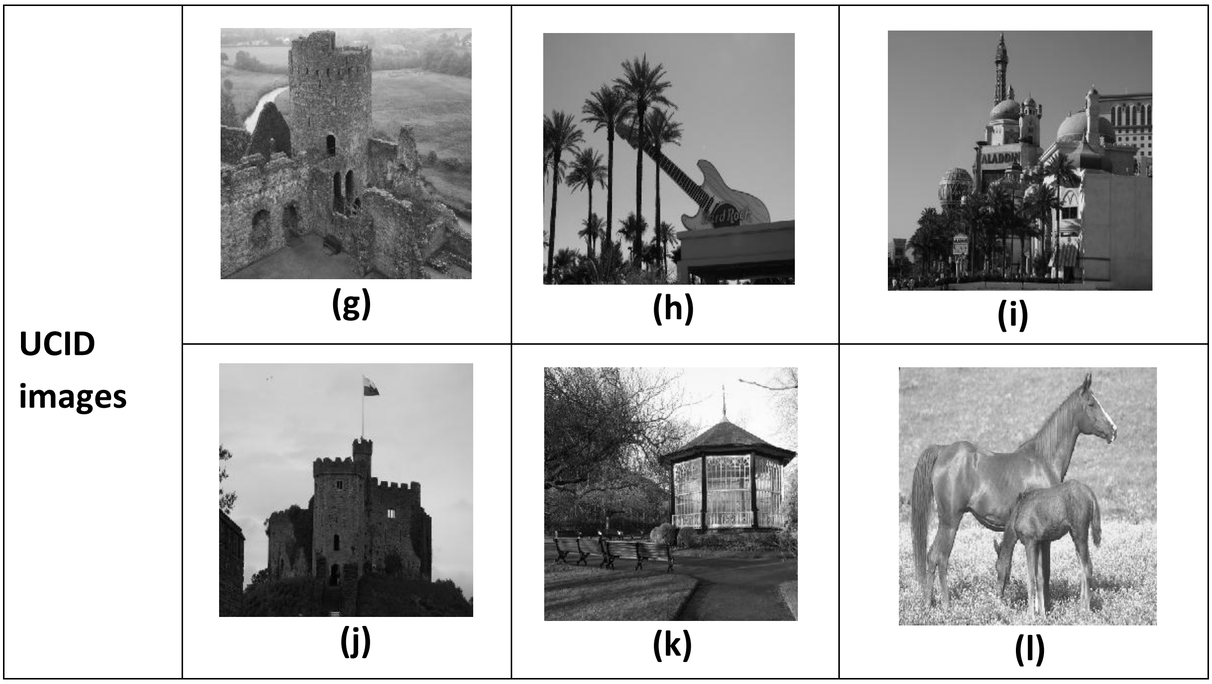


Fig. 8Stego images (512x512) of the proposed scheme (a) Lena (b) Baboon (c) Pepper (d) Lake (e) Tiffany (f) Boat (g) UCID 1 (h) UCID 2 (i) UCID 3 (j) UCID 4 (k) UCID 5 (l) UCID 6

We also analyzed our proposed scheme with some standard statistical parameters like Standard Deviation (SD) and Correlation Coefficient (CC). The Standard Deviation (SD) and Correlation Coefficient (CC) between cover and stego image have been depicted at Table 2. The average Standard Deviation (SD) of cover image and stego image is 45.86 and 45.95 respectively. So, their difference is 0.09 which shows less magnitude change between cover and stego image. The average Correlation Coefficient (CC) between cover and stego image is 0.99 which shows high similarity between cover and stego image.

The performance of the proposed scheme has been analyzed by comparing with other schemes such as Lee & Huang [13] scheme, Tang et. al [14] scheme, and Hu & Li [16] scheme as shown in Table 3.It is clear from the table that the range of PSNR value of Lee & Huang is 31.08 dB to 33.92 dB whereas the range of PSNR value of stego image of Tang et. al is 28.35 dB to 31.60 dB and Hu & Li is 28.33 dB to 29.81 dB. In the proposed scheme, the PSNR value of stego image varies from 34.18 dB to 35.96 dB which shows better image quality than other state-of-the-art schemes.

Table 1: Experimental results of PSNR (dB), SSIM, Q-index, Payload of proposed scheme

Image database	Images (512x512)	PSNR (dB)	SSIM	Q-index	Payload (bpp)
USC-SIPI	Lena	35.96	0.92	0.94	1
	Baboon	34.56	0.91	0.93	1
	Pepper	35.00	0.92	0.94	1
	Lake	35.59	0.93	0.93	1
	Tiffany	35.62	0.92	0.93	1
	Boat	35.70	0.92	0.94	1
UCID	UCID 1	35.89	0.93	0.93	1
	UCID 2	34.98	0.94	0.93	1
	UCID 3	34.88	0.93	0.94	1
	UCID 4	35.04	0.92	0.94	1
	UCID 5	34.18	0.91	0.93	1
	UCID 6	35.13	0.92	0.93	1

Table 2: Standard Deviation (SD) and Correlation Coefficient (CC) of the proposed scheme

Image database	Images (512x512)	SD of Cover image	SD of Stego image	CC between cover and stego image
USC-SIPI	Lena	45.73	45.89	0.99
	Baboon	44.83	44.90	0.99
	Pepper	45.00	45.21	0.98
	Lake	44.73	44.87	0.99
	Tiffany	44.88	44.93	0.99
	Boat	45.68	45.96	0.98
UCID	UCID 1	46.72	46.83	0.99
	UCID 2	46.20	46.32	0.98
	UCID 3	46.35	46.45	0.99
	UCID 4	45.40	45.85	0.99
	UCID 5	46.32	46.23	0.98
	UCID 6	45.33	45.77	0.99

Table 3: Comparison of proposed scheme with state-of-the-art schemes in terms of PSNR value

Image database	Images (512x512)	Lee & Huang [13]	Tang et. al [14]	Hu & Li [16]	Proposed
	Lena	32.85	29.12	28.99	35.96
	Baboon	33.76	31.01	29.81	34.56
	Pepper	33.82	29.44	28.44	35.00
	Lake	31.08	30.34	29.04	35.59

USC-SIPI	**Tiffany**	**32.18**	**28.35**	**28.64**	**35.62**
	Boat	**32.41**	**31.08**	**28.72**	**35.70**
UCID	**UCID 1**	**33.32**	**29.04**	**28.75**	**35.89**
	UCID 2	**32.98**	**29.76**	**29.12**	**34.98**
	UCID 3	**33.12**	**30.10**	**29.08**	**34.88**
	UCID 4	**32.58**	**31.60**	**29.71**	**35.04**
	UCID 5	**32.15**	**30.18**	**28.33**	**34.18**
	UCID 6	**33.92**	**29.05**	**29.40**	**35.13**

5. Conclusion

In this paper, a novel high capacity and low distortion reversible data hiding technique using bit-reversal permutation has been proposed. Here, the secret data is embedded in the cover image by X-OR operation followed by bit reversal permutation. To enhance the security and robustness of the proposed scheme, secret message has been encrypted before embedding into the cover image. The experimental results show that the efficiency of the proposed scheme is very high than previous schemes. As a future work, the proposed scheme can be analyzed against different attacks and can be implemented on frequency domain.

References:

[1] Jana, M., & Jana, B. (2020). An Improved Data Hiding Scheme Through Image Interpolation. In Computational Intelligence in Pattern Recognition (pp. 157-169). Springer, Singapore.

[2] Kankana, D., &Biswapati, J. (2021). A Robust Audio Authentication Scheme Using (11, 7) Hamming Error Correcting Code. In Proceedings of International Conference on Frontiers in Computing and Systems (pp. 671-680). Springer, Singapore.

[3] Jana, M., & Jana, B. (2021). A new DCT based robust image watermarking scheme using cellular automata. Information Security Journal: A Global Perspective, 1-17.

[4] Hassan, F. S., &Gutub, A. (2021). Efficient Image Reversible Data Hiding Technique Based on Interpolation Optimization. Arabian Journal for Science and Engineering, 1-16.

[5] Govind, P. S., Varghese, B. M., & Judy, M. V. (2021). A high imperceptible data hiding technique using quorum function. Multimedia Tools and Applications, 80(13), 20527-20545.

[6] Manasi, J., &Biswapati, J. (2021). Authentication on Interpolated Subsampled Based Image Steganography Exploiting Secret Sharing. In Proceedings of International Conference on Frontiers in Computing and Systems (pp. 681-690). Springer, Singapore.

[7] Atta, R., Ghanbari, M., & IEEE, L. F. (2021). A high payload data hiding scheme based on dual tree complex wavelet transform. Optik, 226, 165786.

[8] Hu, Y., Lee, H. K., & Li, J. (2008). DE-based reversible data hiding with improved overflow location map. IEEE Transactions on Circuits and Systems for Video Technology, 19(2), 250-260.

[9] Tian, J. (2003). Reversible data embedding using a difference expansion. IEEE transactions on circuits and systems for video technology, 13(8), 890-896.

[10] Jung, K. H., &Yoo, K. Y. (2009). Data hiding method using image interpolation. Computer Standards & Interfaces, 31(2), 465-470.

[11] Luo, T., Jiang, G., Yu, M., &Gao, W. (2015). Novel prediction error based reversible data hiding method using histogram shifting. International Journal of Computer Theory and Engineering, 7(5), 332.

[12] Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. IEEE Transactions on circuits and systems for video technology, 16(3), 354-362.

[13] Lee, C. F., & Huang, Y. L. (2012). An efficient image interpolation increasing payload in reversible data hiding. Expert systems with applications, 39(8), 6712-6719.

[14] Tang, M., Hu, J., & Song, W. (2014). A high capacity image steganography using multi-layer embedding. Optik, 125(15), 3972-3976.

[15] Rubio, M., Gómez, P., &Drouiche, K. (2002). A new superfast bit reversal algorithm. International Journal of Adaptive Control and Signal Processing, 16(10), 703-707.

[16] Hu, J., & Li, T. (2015). Reversible steganography using extended image interpolation technique. Computers & Electrical Engineering, 46, 447-455.