Received: 15 February 2018 | Revised: 10 April 2018 | Accepted: 14 May 2018

DOI: 10.4218/etrij.2018-0089

ORIGINAL ARTICLE

WILEY ETRI Journal

High capacity multi-bit data hiding based on modified histogram shifting technique

Nandhini Sivasubramanian | **Gunaseelan Konganathan** | **Yeragudipati Venkata Ramana Rao**

Department of Electronics and Communication, College of Engineering, Guindy, Anna University, Chennai, India

Correspondence
Nandhini Sivasubramanian, Department of Electronics and Communication, College of Engineering, Guindy, Anna University, Chennai, India.
Email: Nandhini2190@gmail.com

A novel data hiding technique based on modified histogram shifting that incorporates multi-bit secret data hiding is proposed. The proposed technique divides the image pixel values into embeddable and nonembeddable pixel values. Embeddable pixel values are those that are within a specified limit interval surrounding the peak value of an image. The limit interval is calculated from the number of secret bits to be embedded into each embeddable pixel value. The embedded secret bits can be perfectly extracted from the stego image at the receiver side without any overhead bits. From the simulation, it is found that the proposed technique produces a better quality stego image compared to other data hiding techniques, for the same embedding rate. Since the proposed technique only embeds the secret bits in a limited number of pixel values, the change in the visual quality of the stego image is negligible when compared to other data hiding techniques.

KEYWORDS
data hiding, embedding capacity, image processing, adaptive embedding, steganography

1 | INTRODUCTION

Data hiding techniques provide a secure means for communication in this digital age. These techniques can be implemented by steganography or cryptography. Cryptography encrypts the host data using a key and produces a noisy form of the host/cover media as the output. The main drawback of this technique is that it lacks data invisibility, meaning that the third party/attacker can clearly understand that secure/confidential data is being sent. Steganography embeds the secret data completely into the host data and produces stego data, which resembles the original host data. Steganography techniques provide data invisibility and have been used since ancient times. Data hiding in images using steganography can be implemented by reversible data hiding and nonreversible data hiding techniques.

Reversible data hiding techniques restore both the cover/host image and the secret data completely at the receiver end. This is basically accomplished by either sharing the values for reversibility through overhead bits/location information bits. Overhead bits are concatenated to the stego image and used at the receiver side. These location information bits are mandatory to completely restore the host image. A reversible data hiding technique with no location information bits greatly improves the efficiency of the algorithm and provides quicker results. Existing irreversible data hiding/data hiding techniques can be divided based on the domain of implementation that is through the spatial and transform domain. The primitive spatial domain-based data hiding technique hides the secret data in the least significant bit of the cover image, called the LSB substitution technique [1]. The drawback is that the stego image was found to be vulnerable to statistical analysis-based attacks [2]. Later, although the revisited LSB matching technique [3] improved the embedding capacity and visual quality

when compared to other LSB-based techniques, it compromised the security of the stego image. By exploiting the modification direction of the above scheme efficiently [4], EMD was proposed, which was found to perform better in terms of embedding capacity and visual quality of the stego image compared to other data hiding schemes. Many variations of the EMD scheme have been proposed [5–9]. A novel data hiding technique using Sudoku [10] was proposed by Chang and others. It uses Sudoku, which is a 9×9 puzzle containing nine 3×3 sub matrices. The secret message is converted into a base 9 numeral using the Sudoku matrix, and is then used for embedding in the cover image. This provided added security to the secret data, and was found to perform better in terms of embedding capacity when compared to the Mielikainen's method and the Zhang and Wang's method [4]. A data hiding scheme based on PVD, named pixel value differencing, was proposed by Wu and Tsai [11], which took human visual characteristics into account. The edges of the grayscale images, rather than the smooth part, were used to hide the secret data. Improvisations of the PVD scheme have been proposed, such as three bit PVD, combining PVD with modulus functions [12,13], and combining PVD with improvised EMD [14]. These techniques focus on improving the embedding capacity and the visual quality of the stego image. Transform domain methods hide the secret data in the DCT or DWT transform coefficients of the image [15–17]. The stego image is formed by applying the inverse transform to the secret data embedded cover image.

The literature survey of data hiding techniques concentrates on improving the embedding capacity of the cover image or the visual quality of the stego image. The proposed technique, which is shown by the flowchart in Figures 1 and 2, introduces the performance measure of recovered cover image quality to study the impact of the data hiding scheme on the cover image. By combining multi-bit secret data hiding with a modified histogram shifting scheme, the proposed technique attempts to balance both embedding capacity and visual quality of the stego image.

2 | FRAMEWORK OF THE PROPOSED TECHNIQUE

2.1 | Preprocessing of the cover image

Assume cover images (X) of size $M \times M$. The peak value P from the cover image histogram is determined by

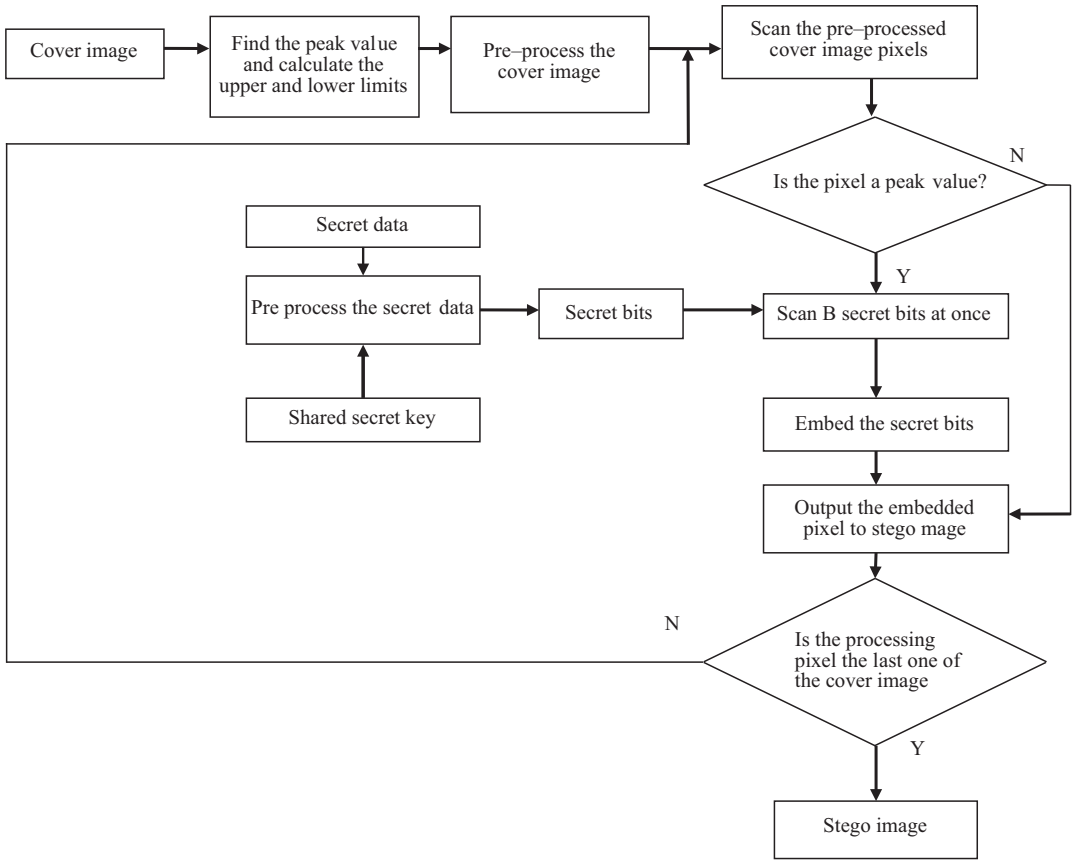

FIGURE 1 Flowchart for the proposed embedding technique

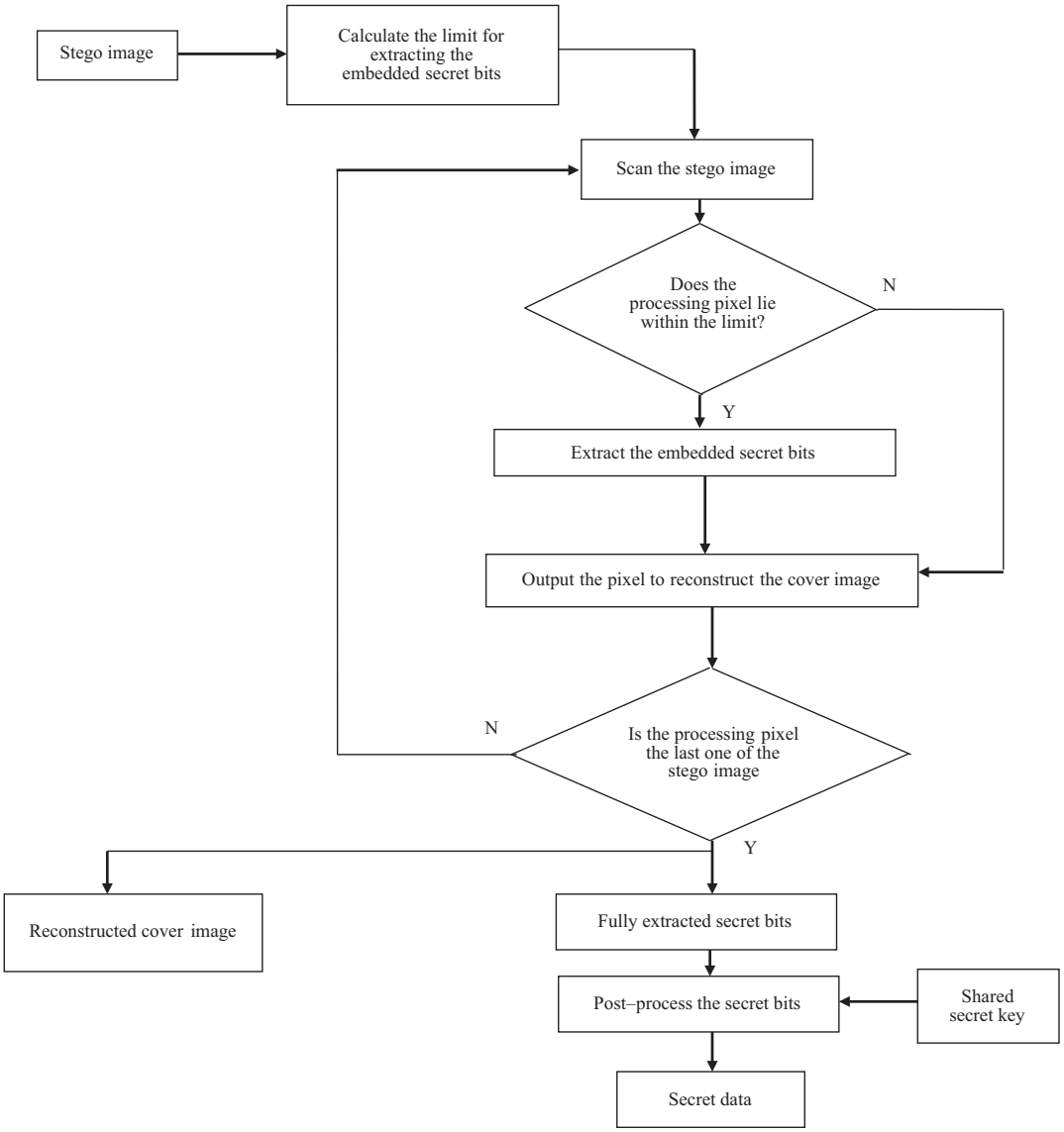

FIGURE 2 Flowchart for the proposed extracting technique

ascertaining the pixel value with the maximum number of occurrences. In order to determine the range of pixel values about P that are to be embedded with the secret bits, A_U and A_L, representing the upper and lower limit of the range are calculated according to (1) and (2), respectively. The cover image X is preprocessed according to (3).

$$A_U = P + (2^B/2), \tag{1}$$

$$A_L = P - ((2^B/2) - 1), \tag{2}$$

$$X' = \begin{cases} P & \text{if } A_U \le X_{i,j} \le A_L \\ X_{i,j} & \text{otherwise} \end{cases} \tag{3}$$

where B represents the number of secret bits inserted into a preprocessed pixel present in the range $[A_L, A_U]$, and X' denotes the preprocessed cover image used for embedding the secret bits.

2.2 | Preprocessing of the secret data

To increase the capacity and security of the secret data that is being embedded, preprocessing of the secret data is carried out. Successive group differencing, followed by Huffman coding, is employed to compress the secret data. Successive group differencing is performed with a shared secret key to increase the security of the secret data. Let K be the shared secret key between the transmitter and receiver, where $K \in [0,255]$. Secret data (ie, the secret image) is converted into a vector (I), which is used for successive group differencing using the shared key K, which is represented in (4)

$$I_j' = \begin{cases} I_j - K & \text{if } j = 1 \\ I_{j-1} - I_j & \text{otherwise.} \end{cases} \quad (4)$$

This is followed by Huffman coding to convert I' into secret bits H. The combined technique of successive group differencing and Huffman coding to convert secret data into secret bits is referred to as preprocessing of the secret data.

2.3 | Proposed embedding technique

The proposed embedding technique to form Stego image Y is explained as follows:

Step 1: Assign preprocessed cover image X' to Y.

Step 2: Secret bits H are processed by grouping B bits at every instant, and are converted to their equivalent decimal value S. In order to embed S, determine lower (S_U) and upper (S_L) limits using (5) and (6), respectively

$$S_U = 2^B - 1, \quad (5)$$

$$S_L = \left(2^B/2\right) - 1. \quad (6)$$

Step 3: Scan the preprocessed cover image pixels and when $Y_{i,j} = P$, go to step 4. Else, go to step 5.

Step 4: Scan the values in S sequentially. Based on the value S, the peak values are modified according to (7).

$$\begin{aligned} &\text{if } (S = 0) \\ &\text{then } Y_{i,j} = P_{i,j} \\ &\text{elseif } (S \in [1, S_L]) \\ &\text{then } Y_{i,j} = P_{i,j} - S \\ &\text{else } (S \in [S_L + 1, S_U]) \text{ then} \\ &S = S - (2^B/2) + 1, Y_{i,j} = P_{i,j} + S \\ &\text{end.} \end{aligned} \quad (7)$$

Step 5: Retain the original pixel value and repeat step 3 until all pixels are processed in Y.

2.4 | Proposed Extracting Technique

At the receiver side, A_U and A_L values are calculated, which will determine the interval in which the secret bits are stored. The secret data is extracted from the stego image using the proposed extraction technique, which is explained below:

Step 1: Determine the number of secret bits embedded pixels (T) using P, A_U, and A_L.

Step 2: If any of the stego image pixels falls within the interval [A_L, A_U], go to step 3. Else, go to step 4.

Step 3: Based on the stego pixel value, secret bits are extracted and stored in the vector R using (8), as follows:

$$\begin{aligned} &\text{for } q = 1 : T \\ &\quad \text{if } (Y_{i,j} = P) \\ &\quad R(T) = Y_{i,j} - P \\ &\quad \text{elseif } \left(Y_{i,j} \in [P + 1, A_U]\right) \\ &\quad R(T) = (Y_{i,j} - P) + (2^B/2) - 1 \\ &\quad \text{elseif } \left(Y_{i,j} \in [A_L, P - 1]\right) \\ &\quad R(T) = \left|Y_{i,j} - P\right| \\ &\quad \text{end} \\ &\text{end} \end{aligned} \quad (8)$$

Step 4: Retain the original pixel value and repeat steps 2 and 3 until all pixels are processed in Y.

Step 5: The cover image X' of size $M \times M$ is extracted from the stego image by shifting the stego image pixels falling within the interval [A_L, A_U] to P.

Step 6: R is converted into its B bit representation, and is decompressed using Huffman decoding to form I'.

Step 7: The final step is successive group addition with shared key K using (9) to form the fully extracted secret data. This procedure is as follows:

$$I_j = \begin{cases} I'_j + K & \text{if } j = 1 \\ I_{j-1} - I'_j & \text{otherwise.} \end{cases} \quad (9)$$

2.5 | Example

To illustrate the proposed data embedding technique, consider $B = 2$, and let the peak value of the histogram P be 150. A_U and A_L are calculated using (1) and (2), which are 152 and 149, respectively. Let the original cover image pixel values be 149, 150, 151, 152, 138, and so on. The preprocessed cover image pixels are calculated using (3), as 150, 150, 150, 138, 150, and so on. Let the secret bits H, obtained after applying the proposed preprocessing technique to the secret data, be 001011011011, and so on. Since the assigned value for B is 2, the secret data is processed in groups of two bits and converted to their corresponding decimal value S. Using the proposed data embedding technique, secret bits are embedded according to (7). The corresponding stego values are shown in Table 1. The corresponding stego image Y pixels after embedding H are 150, 149, 151, 152, 138, and so on. This

process is repeated until all rows and columns of the preprocessed cover image are covered. At the receiver end, A_L and A_U are calculated, which are 149 and 152, respectively. Applying the proposed extracting technique (8), the embedded secret bits from the stego image pixels are extracted. Using the same table, the secret bits R extracted from the stego pixels are 00101101, and so on. This process is repeated for the entire stego image to extract the complete secret bits R. It is decompressed using Huffman decoding and successive pixel addition is performed with shared key K, to form the fully extracted secret data I.

3 | RESULTS AND DISCUSSION

Some of the cover images of size 512 × 512 used for testing the proposed technique are shown in Figure 3. To compare the performance of the proposed technique with that of the existing data hiding techniques, the capacity and peak signal to noise ratio (PSNR) of the stego image are calculated for varying values of B. The embedding capacity of an image is the number of bits that can be embedded into an image. For a given B, the embedding capacity of the cover image depends on the number of pixels between A_U and A_L.

The PSNR value, which is calculated using (10), is the peak signal to noise ratio, which is calculated between the stego image and the original cover image. The PSNR value decides the visual quality of the stego image. The higher the PSNR value, the less noise that is present in the stego image. As a result of this, the stego image is less suspicious. To prove the feasibility of the proposed technique for a wide range of applications, PSNR is also calculated between the extracted cover image and the original cover image.

$$PSNR = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right) \tag{10}$$

where,

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M}(X_{i,j} - Y_{i,j})^2}{M \times M}$$

is the mean square error. An analysis of the proposed technique for varying values of B is shown in Table 2. As the value of B decreases, the PSNR value increases, and correspondingly, the embedding capacity reduces. This is because, the number of nonembeddable pixels decreases, which increases the visual quality. To find the maximum number of bits that can be embedded into the cover image, the maximum embedding capacity (M) is calculated using (11). In (11), B represents the number of secret bits inserted into a preprocessed cover pixel present in the interval $\{V : a \le V \le b\}$, where $a = A_L$ and $b = A_U$, and $N(V)$ represents the number of occurrences of the pixel V in the original cover image.

$$M = B \times \left(\sum_{V=a}^{b} N(V)\right). \tag{11}$$

3.1 | Visual quality evaluation

To evaluate the performance of the proposed technique in terms of the PSNR of the stego image, secret data was considered in the form of images. The size of all cover images and secret images were 512 × 512. The imperceptibility (PSNR) benchmark for the watermarked image is 38 dB [21]. When the proposed technique was tested with different combinations of cover images and secret images, the PSNR value exceeded the acceptable value and was found to perform better when compared with Lee's scheme, which is shown in Table 3. This is because the number of modified pixels in the stego image, in comparison to the cover image, is very low. The proposed technique also outperforms Lee's scheme in terms of the recovery of the secret image, which is shown in Table 4. The checkpoint in Lee's scheme [18] is that the size of the secret data should be equal or less than the embedding capacity of the cover image. In the proposed technique, through a combination of successive pixel differencing with a shared secret key and Huffman coding, the size of the secret bits generated is less than the embedding capacity of the cover image, which is shown in Table 5. This ensures the complete reconstruction of the secret image at the receiver end with infinite dB.

3.2. | Embedding capacity evaluation

In order to evaluate the embedding capacity of the cover image, various values of B were considered. As B was

TABLE 1 Embedding and extraction of secret bits using the proposed technique

Cover image pixels	Secret bits	Corresponding decimal values of the secret bits	Stego image pixels	Extracted secret bits	Corresponding binary values of the secret bits	Extracted cover image pixels
149	00	0	150	0	00	150
150	01	1	149	1	01	150
151	10	2	151	2	10	150
152	11	3	152	3	11	150

FIGURE 3 Some of the cover images used for testing: (A) baboon, (B) peppers, (C) lena, (D) goldhill, (E) fishing boat, and (F) barbara

TABLE 2 Comparison of *M* (bits) and PSNR values (dB) for different values of *B* using the proposed technique

	B = 2		*B* = 3		*B* = 4		*B* = 5		*B* = 6	
Images	***M* (bits)**	**PSNR (dB)**	***M* (bits)**	**PSNR (dB)**	***M* (bits)**	**PSNR (dB)**	***M* (bits)**	**PSNR (dB)**	***M* (bits)**	**PSNR (dB)**
Lena	21,380	61.04	60,819	52.14	151,248	43.53	337,455	37.08	706,434	33.07
Baboon	21,760	60.87	64,095	51.88	163,372	42.91	364,245	35.87	756,006	31.57
Airplane	61,176	56.80	164,220	48.33	399,576	39.61	800,845	33.42	1,114,002	31.12
Sailboat	28,610	59.82	80,433	51.04	178,440	42.72	332,660	36.43	569,538	32.87
Peppers	22,702	61.10	65,901	52.08	156,372	43.80	309,785	37.71	537,054	33.79
Barbara	18,048	61.97	52,788	52.83	132,284	44.20	280,790	37.55	584,700	33.62
Goldhill	19,876	61.58	58,833	52.39	154,096	43.40	358,370	36.65	747,144	32.52

increased from 2 to 6, the maximum embedding capacity of the cover image using the proposed technique increased from 21,380 to 7,06,434 bits when the cover image used was Lena, as shown in Table 2. Figure 4 compares the performance of the proposed technique with that of Wu's [20] scheme and Zhang's [19] scheme for various embedding rates. The proposed technique was found to perform better because it adaptively modified the cover image pixels according to the secret bits. It is important to note that this embedding capacity represents the number of secret bits after preprocessing.

3.3 | Calculation of *Q*

In order to prove that the visual quality of the stego image closely resembles that of the cover image with increasing

TABLE 3 Comparison of the PSNR (dB) of the stego image using the proposed technique with Lee's scheme

	Cover images							
	Lena		**Airplane**		**House**		**Tiffany**	
Secret images	**Lee [18]**	**Proposed**	**Lee [18]**	**Proposed**	**Lee [18]**	**Proposed**	**Lee [18]**	**Proposed**
Lena	N/A	N/A	40.04	43.95	41.28	48.89	40.59	44.66
Airplane	39.97	39.84	N/A	N/A	40.70	48.92	40.03	44.66
House	44.63	39.83	45.12	43.95	N/A	N/A	44.04	44.65
Tiffany	39.78	39.83	38.93	43.95	40.52	48.93	N/A	N/A

TABLE 4 Comparison of the PSNR values (dB) of the recovered secret image using Lee's scheme and the proposed technique

Secret image	**Lena**	**Jet**	**House**	**Milk**	**Tiffany**
Secret data size (bytes)	47,040	53,747	22,477	25,355	56,853
Recovered secret image quality [18] in dB	37.24	35.68	42.69	41.76	35.56
Recovered secret image quality (Proposed technique) in dB	Inf	Inf	Inf	Inf	Inf

TABLE 5 Compression that can be achieved using the proposed preprocessing technique and the maximum embedding capacity of the respective cover images

Cover image	No. of secret bits before preprocessing	No. of secret bits after preprocessing	Maximum embedding capacity (bits)
Lena	162,312	21,309	706,434
Baboon	162,312	22,561	756,006
Barbara	162,312	21,917	584,700
Peppers	162,312	21,277	537,054
Goldhill	162,312	21,426	747,144
Average	**162,312**	**21,645**	**613,386**

payload, the universal image quality index (Q), proposed by Wang and Bovik [23], is calculated between the cover image and the stego image. Q is given by (12)

$$Q = \frac{4\sigma_{xy}\bar{X}\bar{Y}}{(\sigma_X^2 + \sigma_Y^2)\left[\bar{X}^2 + \bar{Y}^2\right]} \tag{12}$$

where $\bar{X}$ and $\bar{Y}$ are the mean of the cover image and stego images, respectively, and $M \times M$ is the size of the cover image. The components for calculating Q are given by (13) to (17)

$$\bar{X} = \frac{1}{m \times m}\sum_{i=1}^{m}\sum_{j=1}^{m} X_{ij}, \tag{13}$$

$$\bar{Y} = \frac{1}{m \times m}\sum_{i=1}^{m}\sum_{j=1}^{m} Y_{ij}, \tag{14}$$

$$\sigma_X^2 = \frac{1}{m \times m - 1}\sum_{i=1}^{m}\sum_{j=1}^{m}\left(X_{ij} - \bar{X}\right)^2, \tag{15}$$

$$\sigma_X^2 = \frac{1}{m \times m - 1}\sum_{i=1}^{m}\sum_{j=1}^{m}\left(X_{ij} - \bar{X}\right)^2, \tag{16}$$

$$\sigma_{xy} = \frac{1}{m \times m - 1}\sum_{i=1}^{m}\sum_{j=1}^{m}\left(X_{ij} - \bar{X}\right)\left(Y_{ij} - \bar{Y}\right). \tag{17}$$

Q represents the difference between two images, and it ranges between −1 and 1. The closer it is to 1, the more similar are the two images. It can be inferred from Table 6 that for lower values of B, the visual quality of the stego image almost resembles the visual quality of the cover image. This accounts for the superior performance of the proposed scheme in terms of perceptual invisibility of the stego image for increased payload.

3.4 | Recovering the cover image

The PSNR of the extracted cover image at the receiver side for various values of B is shown in Table 7. It can be inferred from the aforementioned table that the PSNR values exceed the acceptable values [21]. The number of

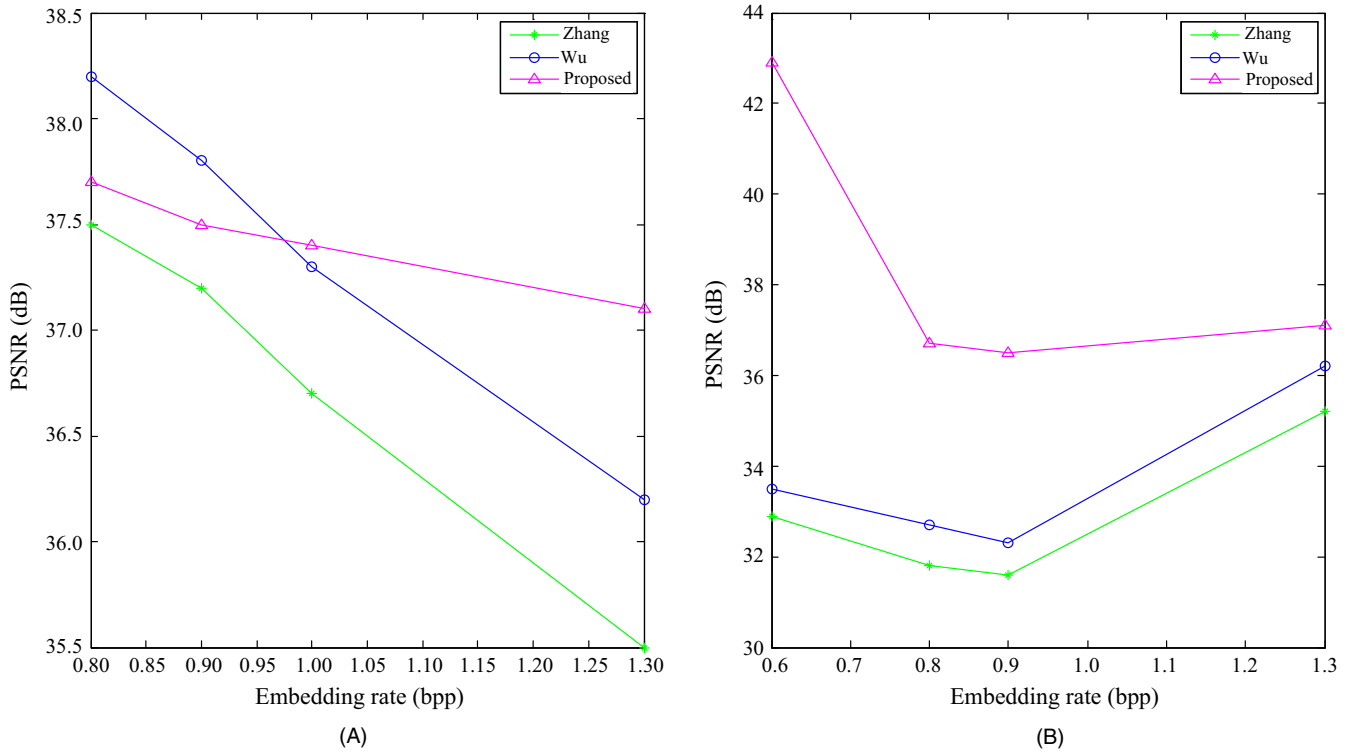

FIGURE 4 Comparison of embedding rate vs PSNR for (A) lena image and (B) baboon image

TABLE 6 Comparison of the Q values of various schemes with the proposed scheme

	Chang et al. [24]		Lu et al. ($\|B\| = 4$) [25]		Lu et al. ($\|B\| = 8$) [25]		Proposed		
Cover image	Q ($T = 15$)	Q ($T = 42$)	Q ($T = 3$)	Q ($T = 18$)	Q ($T = 3$)	Q ($T = 18$)	Q ($B = 6$)	Q ($B = 2$)	Q ($B = 3$)
Lena	0.9951	0.9914	0.9978	0.9943	0.9934	0.9910	0.9959	1.0000	1.0000
Baboon	0.9913	0.9297	0.9955	0.9807	0.9858	0.9768	0.9978	1.0000	1.0000
Pepper	0.9960	0.9892	0.9983	0.9963	0.9951	0.9938	0.9871	1.0000	1.0000
Airplane	0.9948	0.9815	0.9971	0.9923	0.9914	0.9863	0.9984	1.0000	1.0000

TABLE 7 Comparison of the PSNR values (dB) of the extracted cover image using the proposed technique for varying values of B

Images	$B = 2$	$B = 3$	$B = 4$
Lena	61.10	52.20	43.56
Baboon	60.92	51.93	42.96
Barbara	62.03	52.89	44.10
Peppers	61.15	52.13	54.35
Cameraman	59.23	53.60	57.95
Goldhill	61.63	52.388	53.51

overflow/underflow bits of the proposed technique is compared with [14] in Table 8. The added advantage of eliminating the overflow/underflow problem by the proposed technique and the superior recovered cover image quality makes it suitable for medical and military applications.

TABLE 8 Comparison of the number of overflow/underflow pixels of the proposed scheme with [14]

	Number of overflow/underflow pixels	
Cover image	Shen et al. [14]	Proposed
Baboon	53	0
Barbara	6	0
Boat	2	0
House	3	0
Lena	0	0
Goldhill	0	0

Lastly, Table 9 highlights the parameters of the proposed data hiding technique when compared to the existing data hiding techniques, such as SVD-based schemes [22], EMD-based schemes [5], and PVD-based schemes [14], indicating the superior performance of the proposed technique.

4 | CONCLUSION

A novel data hiding technique combining multi-bit data hiding and modified histogram shifting is proposed. On comparing the simulated results of the proposed technique with various data hiding techniques, it is found that there is an improvement in the visual quality of the stego image as the embedding rate is increased. Furthermore, the proposed technique has many features, including the absence of overhead bits, avoiding the overflow/underflow problem, randomizing the secret bits before embedding, and introducing a new performance measure for extracted cover image PSNR at the receiver end. The proposed technique balances the steganography triangle of robustness, security, and capacity by improving the visual quality of the stego image for an increased embedding capacity, and by providing security to the secret data by randomizing it through a combined technique of successive pixel differencing and Huffman coding. Our future work will be to modify the proposed technique in order to extract the cover image losslessly at the receiver side.

TABLE 9 Comparison of different parameters of the proposed technique with various data hiding schemes

Parameters	EMD-based scheme [5]	PVD-based scheme [14]	SVD-based scheme [22]	Proposed scheme	Inference
Stego image quality (dB)	30–53	42	54	31–61	Table 2
Extracted cover image quality (dB)	N/A	N/A	N/A	31–61	Table 7
Randomizing the secret bits before embedding	No	No	No	Yes	Figure 1
Overflow/underflow problem	Yes	Yes	No	No	Table 8
Processing domain	Spatial domain	Spatial domain	Transform domain	Spatial domain	N/A
Embedding capacity (bpp)	1–5	1.6	8	1–5	Table 2
Extraction of the secret data	Lossless	Lossless	Lossy	Lossless	Table 4
Anti-attack ability	No	No	Yes	Yes	Table 6

ORCID

Nandhini Sivasubramanian http://orcid.org/0000-0002-9079-2616

REFERENCES

1. C. K. Chan et al., *Hiding data in images by simple LSB substitution*, Pattern Recog. **37** (2004), 469–474.
2. J. Fridrich et al., Reliable detection of LSB steganography in color and grayscale images, *Int. Conf. Multimedia Security: New Challenges*, Ottawa, Canada, Oct. 2001, pp. 27–30.
3. J. Mielikainen, *LSB matching revisited*, IEEE Signal Process. Lett. **13** (2006), no. 5, 285–287.
4. X. Zhang and S. Wnag, *Efficient steganographic embedding by exploiting modification direction*, IEEE Commun. Lett. **10** (2006), no. 11, 781–783.
5. H. Hajizadeh, A. Ayatollahi, and S. Mirzakuchaki, A new high capacity and EMD-based image steganography scheme in spatial domain, *Iranian Conf. Electrical Eng.*, Mashhad, Iran, May 2013, pp. 1–6.
6. T. D. Kieu and C. Chang, *A steganographic scheme by fully exploiting modification directions*, Expert Syst. Appl. **38** (2011), no. 8, 10648–10657.
7. J. H. Kim et al., *Improved modification direction methods*, Comput. Math. Appl. **60** (2010), no. 2, 319–325.
8. C. F. Lee, Y. R. Wnag, and C. C. Chang, A steganographic method with high embedding capacity by improving exploiting modification direction, *Int. Conf. Intell. Inform. Hiding Multimedia Signal Process.*, Kaohsiung, Taiwan, Nov. 2007, pp. 497–500.
9. J. Wang et al., *An improved section-wise exploiting modification direction method*, Signal Process. **90** (2010), no. 11, 2954–2964.
10. C. C. Chang, Y. C. Chou, and T. D. Kieu, An information hiding scheme using Sudoku, *Int. Conf. Innovative Comput. Inform. Contr.*, Dalian, Liaoning, China, June 2008, pp. 17–22.
11. D. C. Wu et al., *A steganographic method for images by pixel-value differencing*, Pattern Recog. Lett. **24** (2003), no. 9–10, 1613–1626.
12. J. C. Joo, H. Y. Lee, and H. K. Lee, *Improved steganographic method preserving pixel-value differencing histogram with modulus function*, EURASIP J. Adv. Signal Proc. **2010** (2010), 1–13.
13. C. M. Wang et al., *A high quality steganographic method with pixel-value differencing and modulus function*, J. Sys. Soft. **81** (2008), no. 1, 150–158.
14. S. Y. Shen and L. H. Huang, *A data hiding scheme using pixel value differencing and improving exploiting modification directions*, Comput. Security **48** (2015), 131–141.
15. B. Kaur, A. Kaur, and J. Singh, *Steganographic approach for hiding image in DCT domain*, Int. J. Adv. Eng. Technol. **1** (2011), 72–78.
16. C. C. Lin and P. F. Shiu, *High capacity data hiding scheme for DCT-based images*, J. Inform. Hiding Multimedia Signal Proc. **1** (2010), no. 3, 220–240.
17. B. K. Panigrahi and P. S. Reddy, *High quality high capacity robust DWT based steganography*, Int. J. Innov. Res. Dev. **3** (2014), no. 5, 49–52.
18. Y. P. Lee et al., *High-payload image hiding with quality recovery using tri-way pixel-value differencing*, Inform. Sci. **191** (2012), 214–255.
19. X. Zhang, S. Wnag, and Z. Zhou, *Multibit assignment steganography in palette images*, IEEE Sign. Proc. Lett. **15** (2008), 553–556.
20. H. Z. Wu et al., *Multi-layer assignment steganography using graph-theoretic approach*, Multimedia Tools Appl. **74** (2015), no. 18, 8171–8196.
21. S. Voloshynovskiy et al., *Attacks on digital watermarks: Classification, estimation based attacks and benchmarks*, IEEE Commun. Mag. **39** (2001), no. 8, 118–126.
22. N. M. Makbol and B. E. Khoo, *Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition*, AEU – Int. J. Elec. Commun. **67** (2013), no. 2, 102–112.
23. Z. Wang and A. C. Bovik, *A universal image quality index*, IEEE Sign. Proc. Lett. **9** (2002), no. 3, 81–84.
24. C. C. Chang and T. C. Lu, *A difference expansion oriented data hiding scheme for restoring the original host image*, J. Sys. Soft. **79** (2006), no. 12, 1754–1766.
25. C. T. Lu, C. C. Chang, and Y. H. Huang, *High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting*, Multimedia Tools Appl. **72** (2014), no. 1, 417–435.

AUTHOR BIOGRAPHIES

Nandhini Sivasubramanian received her BE degree in electronics and communication and her ME degree in communication systems from PSG College of Technology, Coimbatore, Tamil Nadu, India in 2011 and 2013, respectively. Currently, she is pursuing her PhD degree in electronics and communication at the College of Engineering Guindy, Anna University, Chennai, India. Her main research interests are digital image processing, information security, and watermarking techniques.

Gunaseelan Konganathan received his BE degree in electronics and communication from PSNA College of Engineering, Tamil Nadu, India, in 2002, and his ME degree in communication systems from PSG College of Technology, Coimbatore, India, in 2005. He received his PhD degree from Anna University, Chennai, in 2010. Presently, he is working as an assistant professor with the Department of Electronics and Communication, College of Engineering, Anna University, Chennai, India. His research interests include digital signal processing and wireless communication systems.

Yeragudipati Venkata Ramana Rao received his BTech degree in electronics and communication from Sri Venkateswara University, Tirupati, Andhra Pradesh, India, in 1985, and his MTech and PhD degrees from the Indian Institute of Technology, Madras, India, in 1987 and 1992, respectively. After a brief stint at the Indian Telephone Industries, Bangalore, India, he worked at the Regional Engineering College, Tiruchirappalli, Tamil Nadu, India, from 1992 to 1993. Since 1994, he has been associated with the Department of Electronics and Communication, College of Engineering, Anna University, Chennai, India, and is currently working there as the Professor. His research interests include digital signal and image processing, VLSI design, and VLSI digital signal processing.