International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient Block Based Self-Secured (BBSS) LSB Embedding Scheme over OFDM Based Wireless Communication Channel

Abhijit S. Mali, Manoj M. Dongre

Submitted: 25/11/2023 **Revised**: 30/12/2023 **Accepted**: 09/01/2024

Abstract: The paper presents an efficient and robust Block Based Self-Secured (BBSS) image steganography approach for secured transmission over OFDM (Orthogonal Frequency Division Multiplexing) based Wireless Communication (WC) Channel. The suggested BBSS scheme uses LSB Embedding (LSB-E) with low computational complexity and maintains a balance between perceptual quality and security. The 9:1 (bytes) embedding scheme finds the initial index position in the 8-neighbours considered clockwise from top left corner of a 3x3 block of the center pixel. The index is function of the magnitude of the center pixel and found using the Natural Logarithm. The proposed embedding scheme is highly immune to any unwanted noise for values of center pixel above 12. The paper evaluates the performance of the proposed BBSS steganography scheme using BPSK (Binary phase shift keying) modulated WC channel with AWGN (Additive White Gaussian Noise) interference. The simulation results showed lossless transmission at 10 dB signal to noise ratio, high PSNR of 51.65 and 99.95% structural similarity between the target and recovered stego image.

Keywords: *Block Based Self-Secured, steganography, OFDM, Wireless Communication, LSB Embedding, Natural Logarithm and AWGN.*

1. Introduction

The objective of image steganography is to hide an image (called secret image) in another image (called cover image) preserving the perceptual quality of the cover image and making any malicious user (intruder) difficult to extract the hidden information (secret image). A robust approach should preserve the contents (stego image) from deterioration and offers low computation cost for embedding and de-embedding. Many state of art work had been published suggesting lossy and lossless steganography schemes but somehow failure resulted due to un-balance between various performance parameters such as capacity, quality, security and noise.

The challenge lies is to offer minimum distortion and contamination of the cover envelop while enclosing the useful private data. The capability of the embedding scheme lies in its mathematical approach used for extracting the information reversibly without any loss, distortion or alignments. The measure of a good steganography approach is determined by the accuracy and data consistency and is seen to remain the basis of today's complex mathematical designs. Many literatures focused on either maximizing capacity through exploiting data redundancy or maintaining imperceptibility using reversible encoding. Various reversible steganography methodologies with principles and applications can be found in [1-11] and [12-20] respectively.

Broad classification of image steganography algorithms includes the spatial domain and the transform domain approaches. Spatial domain methods are the most commonly used algorithms and uses the least significant bit for data hiding. The ratio of hiding is certainly 8:1 (bits) offering lower capacity but requires minimum computations due to their simplicity. As far as perceptual quality of the stego image is concerned, it offers better resemblance between the original cover image and the stego image thus avoiding deterioration and degradation. When propagated over a noisy channel such stego image have low impact on the single embedded LSB bit and can be recovered using any steganalysis algorithm. Due to their simple embedding mechanism they are susceptible to seen or unseen attacks. Some of the common approaches involving the LSB embedding schemes uses histogram alignments, pixel luminance, pixel indexing, random embedding etc. Pixels are transformed using available transforms to obtain new values called coefficients. These transform coefficients are used to embed secret data and are recovered with minimal distortion. Such transform based schemes offers better resistance to external attacks but mostly are non-reversible due to real values of transform coefficients. The reconstruction includes rounding of coefficient values which affects the original secret values as a result of diffusion error. Various expectations of a good quality steganography are mentioned in [21] which dealt with parameters including substantiality, computations,

Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai. Maharashtra, India, 400706, abh.mal.rt21@dypatil.edu, manoj.dongre@ dypatil.edu

perception, capacity and resistance. Recent advances and challenges can be studied from [22].

2. Contributions

The paper contributes on the following aspects:

1. A novel data hiding technique BBSS-LSB using LSB embedding is suggested which offers higher peak signal to noise ratio and structural similarity between the cover and stego images.
2. An OFDM based Wireless Communication model is designed using BPSK Modulation to transmit the stego image over varying noise level in AWGN channel and analyse the effects over received data.
3. The performance of the proposed BBSS-LSB Embedding scheme is compared with recent state of art methods.

3. Related Work

The authors in [23] used LSB, secret key and XOR operation where the secret key is transformed to 1D array and XOR-ed with the secret data. They performed 1-LSB and 4-LSB embedding over grayscale and color images. An image encryption based on hypechaos and compressive sensing is suggested in [23]. A plain image is subjected to discrete wavelet transform (DWT) to generate a sparse matrix and encrypted using a dynamic spiral block scrambling. A cipher image is then obtained by compressing and quantifying the encrypted image. Further the cipher image is converted into meaningful steganography image by embedding it into the alpha channel of the portable network graphics formatted cover image. The scheme offers low transmission cost and storage with high visual security. A chaos based data hiding scheme is introduced in [24]. The method secretly embeds bits in the color image where the destination bits are found using logistic map and the secret channel is selected randomly. The author used four different steganography algorithm over 10 sample images and showed that the scheme provide better security against attacks.

Authors in [25] combined Diffie-Hellman Key Exchange with a modified Collatz Conjecture for generating random numbers to identify the unique destination bit in the cover image for data hiding. Work suggested in [26] used Huffman code, LSB based cover steganography using colourless part and Multilevel Encryption of the picture. A secret key is encrypted using AES encryption followed by compression of the encrypted message using Huffman coding [27]. The author introduced multilayer LSB exchange method (MLLSBEM) modifying the LSB embedding. The scheme ensured a better compromise between security, capacity, imperceptibility and reliability. High imperceptibility and capacity [28] was obtained by compressing the message using LZW coding technique. The compressed bits of the secret image are then embedded in LSB's of the edge pixels of the cover image ensuring the cover image to remain the same after embedding process (the stego image). The location of the embedded bits are maintained in a location file which is used by the receiver to recover the embedded pixels of the secret image.

Work suggested in [29] proposes a LSB matching revisited method a kind of Exploiting Modification Direction (EMD) method that results a minimum modifications to the cover image. The scheme uses modified LSB matching and the EMD method called dual images Reversible Data Hiding for quality image and capacity. A more sophisticated work is carried in [30] where the secret image is transformed to noise vector and then to stegno image using a GAN (Generative Adversarial Network). Further the secret image is extracted by updating noise vector with gradient descent approach. The scheme offers better protection against steganalysis attacks, it suffers from transmission errors. A novel of phase drift based on drift correction in PSK (Phase shift keying) or QAM (Quadrature Amplitude Modulation) was incorporated in dirty constellation was used in [31] for wireless covert channel which was extended from audio watermarking. The secret image is embedded in luminance and chrominance part of the cover image and uses Discrete Cosine and Discrete Wavelet transform [32]. The encryption is carried out using chaotic Baker map, a permutation based algorithm, having good tolerance to channel behaviour. The OFDM based channel equalization system was used for investigating the performance of the proposed steganography approach.

4. Material and Methods

The proposed work makes use of images from distinct datasets shown in figure 1. It consists of 4 target and 4 secret images. The objective behind the use of these images is related to the high coloured graphics used in the secret images and to measure the imperceptibility after data hiding in proportionate background-foreground ratio in the cover image. The images in the dataset carried different dimensions. To reduce the transmission time over the wireless channel, the images were resized to lower resolution. The images were downloaded from KADID-10k IQA Database [33].

Fig 1 – Cover Images (Upper row) and Secret Images (Bottom row) from KADID-10k IQA Database.

The BBSS LSB Embedding scheme ensures the size of the cover image and the secret image. The ratio of embedding is 9:1 bits for the cover and the secret image. The row and column size of the cover image is maintained to be multiple of 3, whereas the row and column size of the secret image is ensured to be exactly divisible by 3. The same is maintained either by removing or adding extra row or column at the end of the cover image and resizing the secret image as per need through Bilinear Interpolation. The following expression (1) gives the relationship:

$D_{cover\ image}$ = *rsize mod 3 and csize mod 3 = 0*

$D_{secret\ image}$ = *rsize mod R and csize mod C = 0*

.....(1)

Where, *rsize & csize* are number of rows and columns of cover image and *R & C* are the row size and column size of the secret image. D_x represents the dimension of either the cover or the secret image.

A 3x3 block of a cover image is shown in the figure 2 below. The proposed BBSS-LSB Embedding scheme consider the center pixel C=115 and the sequence of normal embedding of secret image bits indicated by the arrows and numbered starting from the top-left corner and sequencing right-down-left and then upward.

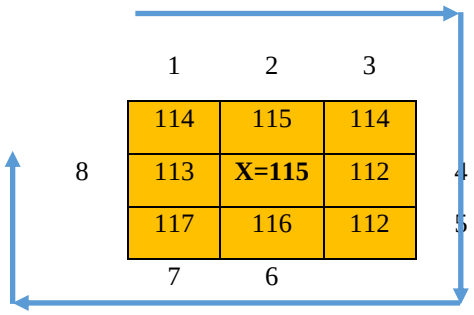

Fig 2 – 3x3 block from the cover image

The BBSS LSB embedding scheme initially finds the starting point from the 8-neighbors from where the first bit will be embedded and follow the normal sequence in clockwise direction as indicated. The initial point is a function of the magnitude of the center pixel and is found from the following logarithmic equation (2).

$$Starting\ Point\ index\ (I) = round(\frac{log\ cp}{log\ 2}) \qquad (2)$$

Where *I*, is the number corresponding to the starting point from where actually the first bit of secret image is to be embedded. The '*log'* in the expression is the natural logarithm, and *cp* is the value of center pixel. Since the values '0' and '1' for the term *log cp* will amount to log (0) = 1 and log (1) = 0, therefore, equation (2) was reduced to following expression (3).

$$I = \begin{cases} 1 & cp == 0 \\ 1 & cp == 1 \\ round(\frac{log\ cp}{log\ 2}) & otherwise \end{cases} \qquad (3)$$

The ratio $\frac{log\ cp}{log\ 2}$ will result in real values which are rounded to nearest integers. For *cp = 0, 1 and 2*, the starting point will be byte 114 at the top left. The second byte 115 at the top middle would serve as the starting point for *cp = 3, 4, and 5* while byte 114 at the top right will be starting point for *cp = 6 to 11*. The change in index with respect to magnitude of the center pixel *cp* is indicated in Table 1.

Table 1 –Index values with respect to magnitude of center pixel cp

cp / Initial index	**1 (MSB)**	**2**	**3**	**4**	**5**	**6**	**7**	**8 (LSB)**
0-2	1	2	3	4	5	6	7	8
3-5	8	1	2	3	4	5	6	7
6-11	7	8	1	2	3	4	5	6
12-22	6	7	8	1	2	3	4	5
23-45	5	6	7	8	1	2	3	4

46-90	4	5	6	7	8	1	2	3
91-181	3	4	5	6	7	8	1	2
182-255	2	3	4	5	6	7	8	1

The center pixel value in the stego image remains unchanged to ensure the perceptual quality of the cover image. If we consider 50% change in the LSB encoding, it would not affect the perceptual quality of the cover image in the stego image. The MSB bit is embedded first and LSB bit of the secret image is embedded at the last. The following figure 3 depicts the scheme of embedding and Algorithm 1 explain the complete procedure of embedding the secret image in the cover image using the BBSS-LSB Embedding scheme.

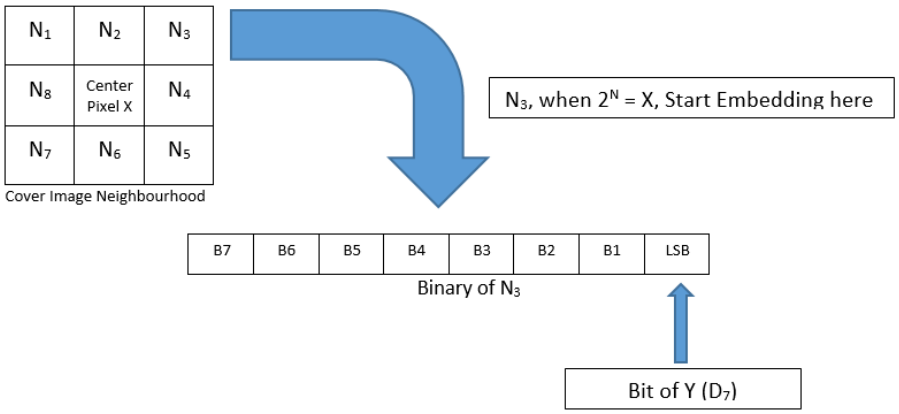

Fig 3 – Secret bit hiding using the proposed BBSS-LSB Embedding scheme

Algorithm 1 – BBSS LSB Embedding Scheme

Input – Cover Image C and Secret Image S

Output – Stego Image SS

Calculate Nr - Number of 3x3 Blocks in first dimension of C

Calculate Nc – Number of 3x3 Blocks in second dimension of C

for m =1 to Nr

for n =1 to Nc

Block B = C(m,n) ; Get the 3x3 block from the cover image C

Cp = B(2,2) ; Get the center pixel

Find index I using equation (2)

Convert byte in secret image to binary - sb

For b = 1 to 8

Convert byte at index I to binary - bb ; refer figure 1

Store secret bit in sb at LSB position (MSB first)

Convert the byte bb back to decimal – store in SS at (m,n)

Point to next byte of BB in clockwise direction

Point to next bit in sb

End loop ; b

Point to next byte in secret image ; S (columns)

End for ; n

End for ; m

Once the stego image is obtained using the SSBB- LSB Embedding scheme, bytes in the stego image is transmitted over the wireless communication channel. The proposed work considered 802.11a model [34] using BPSK modulation with OFDM. The input to the wireless communication system is 24 binary bits (3 bytes) passed through a convolutional encoder thus maintaining a code rate of ½. None of the bits are punctured and the data is interleaved using a matrix interleaver. The output from the BPSK modulator is fed to the OFDM block where extra 4 bits (pilots) are added for desired phase shift along with a zero in the middle. The 48 symbols from the BPSK modulator are partitioned equally by inserting zero in the middle. Further, 24 symbols on each side are portioned using 2 pilots into three segments consisting 6, 13 and 5 symbols from the center. The OFDM produces 53 symbols which are padded with zeros to obtain symbol length of 2^6 = 64 for Inverse fast Fourier transform. A guard band is provided to prevent inter-symbol interference between two channels of size 16. The proceeding 16 symbols in the 64 symbols are concatenated at the end (cyclic prefix) for the guard band making the total bandwidth to cover 80 symbols. The message is transmitted through AWGN channel with varying signal to noise ratio.

The receiver function exactly opposite. The guard band, zero padding, pilots and a zero are removed to obtain the 48 symbols. The symbols are demodulated using a BPSK demodulator, de-interleaved and de-punctured. A Unipolar to Bipolar block and an insert zero block in combination is used as a de-puncturer. The bits are decoded using a Viterbi decoder and compared with the transmitted bits. A bit error block is used to measure the error in transmission due to channel effect. The following simulation model (MATLAB 2021b) shown in the figure 4 represents the wireless communication system for the proposed stego image data transmission.

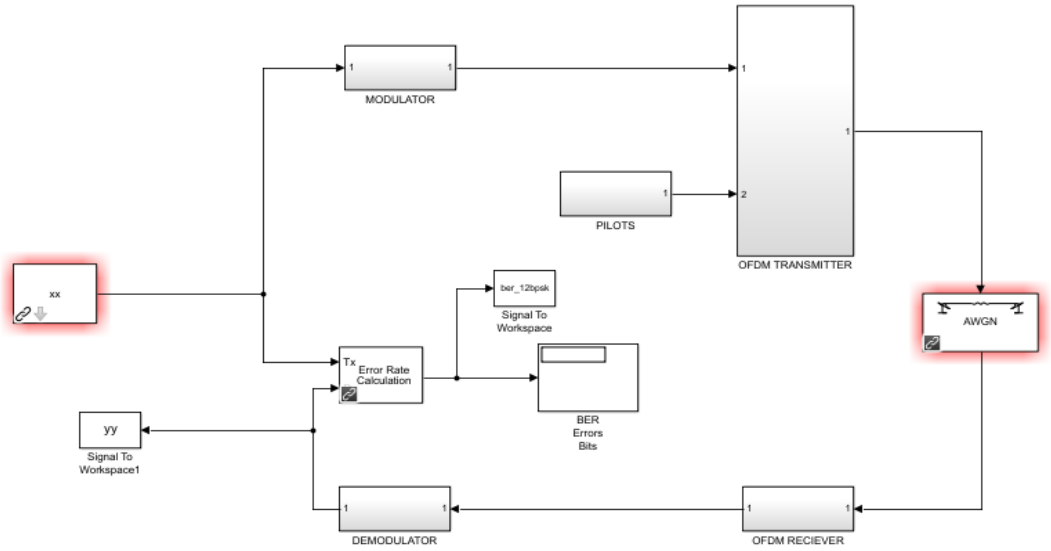

Fig 4 – Simulation Model for Wireless Communication System

The input box shows variable xx and the output block shows variable yy. Both the input and the output have 24 bits. The value of xx is fed through Matlab code and the output is obtained for single run from yy from the workspace. The stego image is partitioned in block of 3 bytes and fed to the system through xx whereas the output is received in yy and stored until all blocks are received. The received blocks are then arranged and resized according to the dimension of the transmitted stego image. The following figure 5 shows the complete block diagram of the BBSS-LSB Embedding scheme based stego image transmission over wireless communication system.

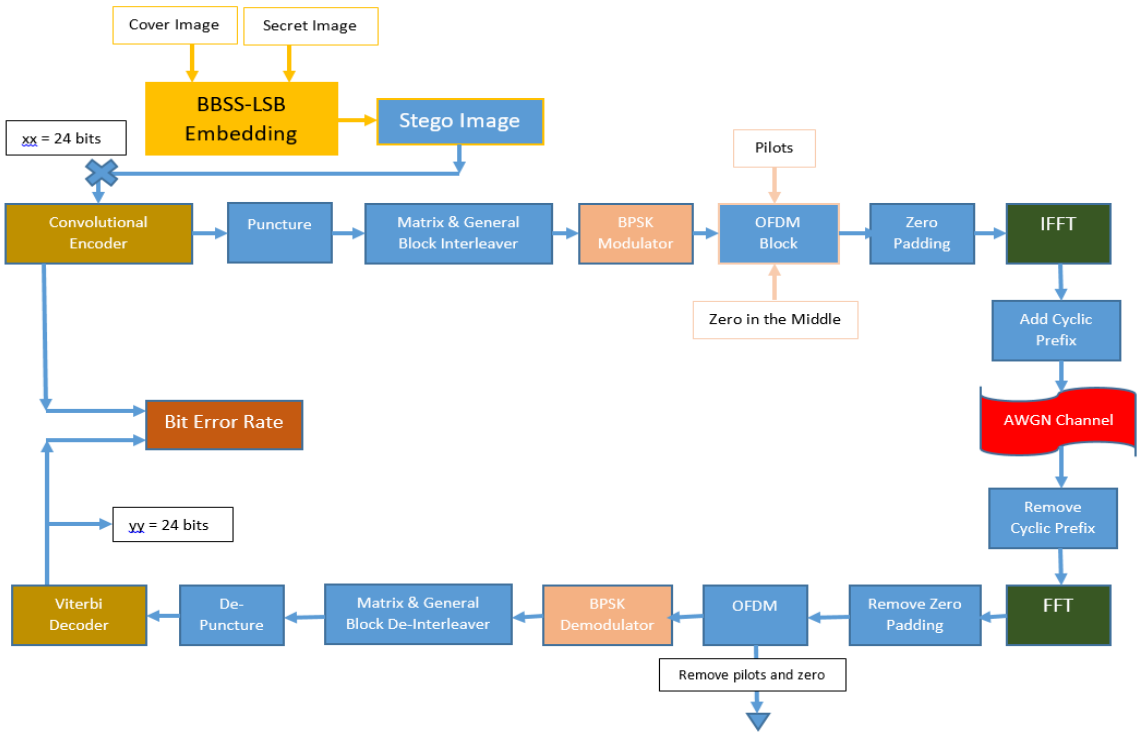

Fig 5 – Complete block diagram for the proposed system

The system is tested for signal to noise ratio (SNR) value in the AWGN block for which the system respond error free reception for randomly transmitted data. It was found that the system was able to receive lossless data at the output for SNR=12 dB (decibels). The system is evaluated for SNR values from 0 to 12 dB at the offset of 2 dB for the same stego image. The values of SNR and Peak SNR are found along with BER (Bit Error Rate). Table 2 below shows the model parameters and their properties.

Table 2 – Model Parameters and values

Wireless Model	802.11a WLAN
Convolutional Encoder	poly2trellis(7, [171 133])
Code Rate	0.5
Puncture Vector	[1 1 1 1 1 1]
Matrix Interleaver	Number of Rows=6, columns=8
Gain	1/sqrt(10)
Pilots (bits)	4
Zero Padding (bits)	11
Cyclic Prefix (bits)	16
Input	24 bits
Input signal power, referenced to 1 ohm (watts) (AWGN)	0.01
Data Rate	6 Mbps

5. Results and Discussion

The following figures from 6 to 10 shows the performance of BBSS-LSB Embedding scheme when transmitted over communication channel with varying values of signal to ration affecting the stego image. The cover image and the secret image are resized to 150 x 210 and 50 x 70 to reduce the simulation time. The secret image is embedded using the proposed BBSS scheme to

obtain the stego image. The stego image is transmitted row wise through the communication system and received at the receiver end. The de-embedding process to embedding is used to obtain to recover the secret image. Figure 4 shows the input and outputs of the steps explained.

Fig 6– Lossless Transmission: (SNR-12dB, BER=0) Cover image, Secret image, resized cover image (150x210) and secret image (50x70), Stego image obtained using BBSS-LSB Embedding scheme, Received stego image from communication system and the recovered secret image.

The value of SNR is varied from 4 dB to 12 dB at an offset of 2 dB and respective stego/secret images at the receiver end are shown in figures from 7 to 10 in reverse order. Table 3 highlights the effect of steganography and communication system. The mean squared error (MSE), Peak signal to noise ratio (PSNR) and structural similarity index measure (SSIM) between the cover image and the stego image (fixed to two digit precision) are 0.44, 51.67 and 0.99956 respectively. Visual perception of the stego image in figure shows that it has greater resemblance to the cover image. Thus, our proposed approach of embedding does not affect the cover image and had 99.95% similarity with stego image with higher PSNR of 51.67. The value of SNR plays important role for the disparities in transmitted stego image and the received stego image and consequently the received cover and the secret image. The MSE and the SSIM increases with decreasing values of SNR eventually decreasing the PSNR. The feasible values of SNR as seen from the performance in Table 3 will be 10 dB and above. The performance can be further improved by channel estimation approaches. The performance of correlated images with respect to MSE, PSNR and SSIM with respect to SNR are depicted in figure 11 to 13.

Fig 7 - Received stego image and Recovered Secret image for SNR=10

Fig 8 – Received stego image and Recovered Secret image for SNR=8

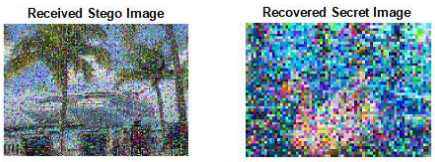

Fig 9 – Received stego image and Recovered Secret image for SNR=6

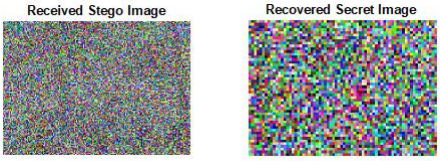

Fig 10 – Received stego image and Recovered Secret image for SNR=4

Table 3 –MSE, PSNR and SSIM for varying SNR values for BPSK system and ½ code rate

SNR-dB	MSE				PSNR				SSIM			
	C-SS	**C-SS$_R$**	**SS$_T$-SS$_R$**	**S-S$_R$**	**C-SS**	**C-SS$_R$**	**SS$_T$-SS$_R$**	**S-S$_R$**	**C-SS**	**C-SS$_R$**	**SS$_T$-SS$_R$**	**S-S$_R$**
12	**0.44**	0.44	0	0	**51.67**	51.67	-	-	**0.99956**	0.99956	1	1
10	**0.44**	0.44	0	0	**51.67**	51.67	-	-	**0.99956**	0.99956	1	1
8	**0.44**	298.99	298.65	372.5	**51.67**	23.37	24.75	22.42	**0.99956**	0.8327	0.82359	0.94298
6	**0.44**	3228.12	3228.5	5590.1	**51.67**	13.04	-35.09	10.67	**0.99956**	0.29964	0.28927	0.46739
4	**0.44**	8168.87	8170.2	11588.6	**51.67**	9.009	-39.92	7.50	**0.99956**	0.03906	0.03082	0.06357

Where ***C - Cover Image, S - Secret Image***

SS - Stego Image

SS$_T$ - Transmitted Stego Image

SS$_R$ - Received Stego Image

S$_R$ - Recovered Secret Image

*Empty cells indicate infinity values**

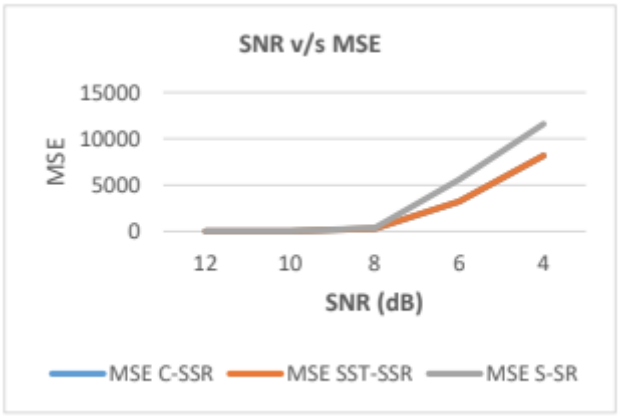

Fig 11 – Mean Squared Error values for Signal to Noise Ratio

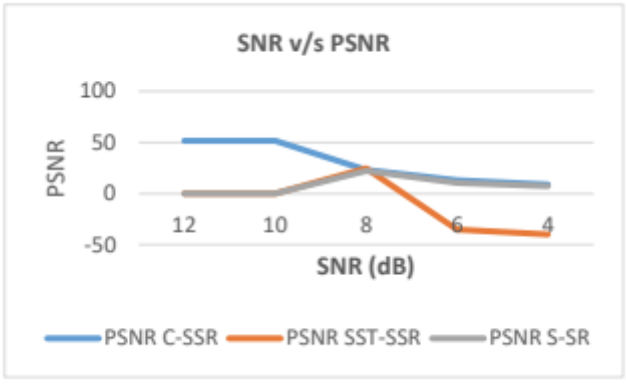

Fig 12 - Peak Signal to Noise Ratio values for Signal to Noise Ratio

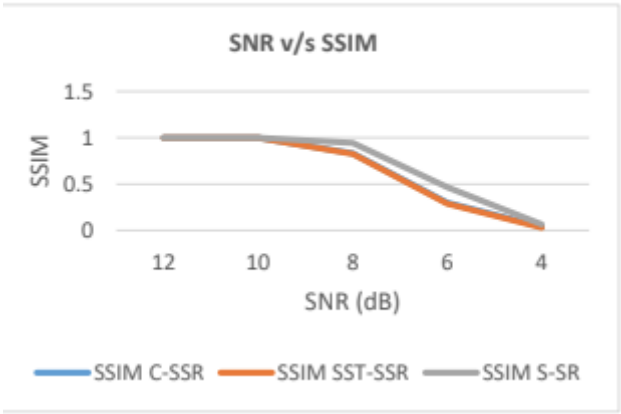

Fig 13– Structural Similarity Index Measure for Signal to Noise Ratio

The performance of the wireless communication system using BPSK modulation scheme for ½ and ¾ code rate with respect to SNR and BER is shown in the figure 14. The BER approaches zero at 12 dB SNR when BPSK is used for ½ code rate, and at 15 dB for code rate of ¾. Therefore the proposed work uses BPSK with ½ code rate. The estimation belonging to SNR below 4 dB is not covered in the table 3 since the received stego image and certainly the recovered secret image are severely deteriorated. The deterioration at SNR=4 dB can be seen from figure 10 where both the images have no resemblance with respect to their original form shown in figure 6. The values of BER are plotted for SNR values ranging from 0 to 12 dB in figure 14. The BER is high at low SNR and decreases when SNR increases.

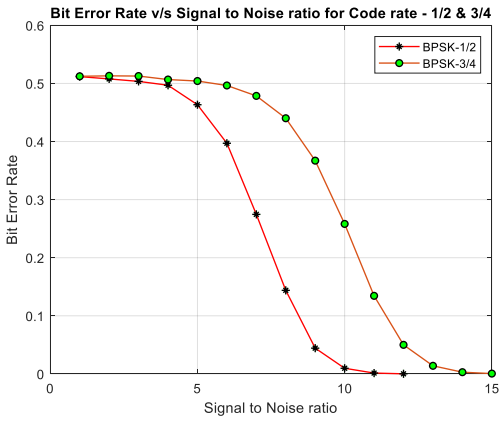

Fig 14– Comparative performance of BPSK Modulation scheme (Code Rate – ½ and ¾)

The proposed BBSS-Embedding scheme is compared with state of art steganography methods including 1-LSB/4-LSB scheme (Sabah A.Jebur et al. 2023), Multi-Layer Least Significant Bit Exchange Method (MLLSBEM) (Rana S. Hameed et al. 2022), encryption using chaotic Baker map (Asmaa A. Eyssa et al., 2020), Rotating & shifting poly-pattern block matrix (Hacimurtazaoglu M. and Tutuncu K., 2022), Adaptive Matrix Pattern (AmirfarhadNilizadeh et al., 2021) and Pixel Value Differencing and Pixel Shifting Technology (Huang, C.T. et al., 2023). Table 4 shows that the MSE and SSIM in case of Multi-Layer Least Significant Bit Exchange Method is minimum while Rotating & shifting poly-pattern block matrix based steganography has highest PSNR. It is seen that there is trade-off between these performance parameters. Different methodologies used different configuration for steganography including number of hidden bytes, cover and secret images, targeted bits to be replaced in the binary bit stream, capacity etc. The comparison parameters in Table 4 are based on different strategies as far as the embedding process is concerned. The proposed scheme tries to maintain a balance between all three parameters and shows better performance with respect to PSNR and SSIM. The performance of the suggested scheme is evaluated with respect to different combinations of target and the secret images. The average values of all three parameters are listed below in Table 5.

Table 4 –Performance comparison of proposed BBSS-LSB Embedding scheme with state of art steganography techniques.

Sr. No.	Reference	MSE	PSNR	SSIM
1	Sabah A. Jebur et al. [21]	3.47	42.75	-
2	Sabah A. Jebur et al. [21]	27.21	29.28	-
3	Rana S. Hameed et al. [27]	0.0149	-	1
4	Asmaa A. Eyssa et al. [32]	-	40.4615	-
5	Murat H. et al. [35]	0.24	54.76	0.998675
6	AmirfarhadNilizadeh et al. [36]	-	54.00	-
7	Cheng-Ta Huang et al. [37]	-	36.60	0.94
8	Proposed BBSS-LSB Embedding	0.44	51.67	0.99956

Table 5 – The overall performance of BBSS-LSB Embedding scheme.

Target Image	Secret Image	MSE	PSNR	SSIM
1	1	0.44	51.66	0.99959
	2	0.44	51.67	0.99959
	3	0.44	51.67	0.99959
	4	0.45	51.64	0.99959
2	1	0.45	51.62	0.99931
	2	0.44	51.65	0.99929
	3	0.44	51.67	0.99930

	4	0.45	51.63	0.99931
3	1	0.44	51.67	0.99955
	2	0.45	51.63	0.99954
	3	0.44	51.67	0.99956
	4	0.45	51.63	0.99955
4	1	0.44	51.65	0.99969
	2	0.44	51.66	0.99969
	3	0.44	51.65	0.99969
	4	0.44	51.65	0.99969
Average		**0.443125**	**51.65125**	**0.999533**

6. Conclusion

The work introduced propose a novel steganography approach using LSB Embedding. The scheme uses the center pixel to find the initial bit embedding position along its neighbour in a 3x3 neighbourhood considered in clockwise direction. The technique is simple, fast, accurate and secured. The BBSS-LSB scheme offers high PSNR of 51.56 and better imperceptibility with 99.95% structural similarity. The limitation of the scheme is its low immunity to noise for low magnitude of center pixel values below 12. A small amount of noise in the center pixel can cause disturbance and affect the starting hidden index for low values. When transmitted over a communication channel, it is seen that it has the ability to sustain noise up to 2 dB (SNR = 12 dB lossless transmission for BPSK and at 10 dB shows similar performance) after which the recovered target image and eventually the secret image deteriorate. The performance of the proposed scheme can be improved through necessary arrangements for value of N=0,1,2 and 3 referred to figure 3. This would definitely improve the MSE and as a result the PSNR value. The system can be tested for different modulation schemes such as QPSK (Quadrature phase shift keying) and QAM (Quadrature Amplitude Modulation).

References

[1] C.-Y. Chang and S. Clark, "Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method," Computational Linguistics, vol. 40, no. 2, pp. 403–448, 2014.

[2] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in Proceedings of the SPIE, vol. 4314, pp. 197–208, San Jose, CA, USA, January 2001.

[3] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 97–105, 2003.

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

[5] M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147–1156, 2004.

[6] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: a new framework and an implementation," IEEE Transactions on Image Processing, vol. 15, no. 4, pp. 1042–1049, 2006.

[7] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 321–330, 2007.

[8] X. Huang, A. Nishimura, and I. Echizen, "A reversible acoustic steganography for integrity verification," in Proceedings of International Workshop on Digital Watermarking (IWDW), pp. 305–316, Seoul, Korea, October 2010.

[9] D. Coltuc, "Low distortion transform for reversible watermarking," IEEE Transactions on Image Processing, vol. 21, no. 1, pp. 412–417, 2012.

[10] W. Zhang, X. Hu, X. Li, and Y. Nenghai, "Optimal transition probability of reversible data hiding for general distortion metrics and its applications," IEEE Transactions on Image Processing, vol. 24, no. 1, pp. 294–304, 2015.

[11] B. Ma and Y. Q. Shi, “A reversible data hiding scheme based on code division multiplexing,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1914–1927, 2016.

[12] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding-a survey,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[13] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.

[14] R. Liu and T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership,” IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128, 2002.

[15] C.-C. Lai and C.-C. Tsai, “Digital image watermarking using discrete wavelet transform and singular value decomposition,” IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, pp. 3060–3063, 2010.

[16] J. Fridrich, “Image watermarking for tamper detection,” in Proceedings of International Conference on Image Processing(ICIP), pp. 404–408, Chicago, IL, USA, October 1998.

[17] D. Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1167–1180, 1999.

[18] T.-Y. Lee and S. D. Lin, “Dual watermark for image tamper detection and recovery,” Pattern Recognition, vol. 41, no. 11,pp. 3497–3506, 2008.

[19] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, “Writing on wet paper,” IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3923–3935, 2005.

[20] V. Holub, J. Fridrich, and T. Denemark, “Universal distortion function for steganography in an arbitrary domain,” EURASIP Journal on Information Security, vol. 2014, no. 1, pp. 1–13, 2014.

[21] Sabah A. Jebur, Abbbas K. Nawar, Lubna E. Kadhim and Mothefer M. Jahefer, “Hiding Information in Digital Images Using LSB Staganography Technique,” iJIM, volume 17, No. 7, 2023.

[22] Jayakanth Kunhoth, Nandhini Subramanian, Somaya Al-Maadeed and Ahmed Bouridane, “Video steganography: recent advances and challenges,” Multimedia Tools and Applications, 2023, https://doi.org/10.1007/s11042-023-14844-w.

[23] Xing-Yuan Wang, Xiao-Li-Wang, Lin Teng, Dong-Hua Jiang and Yongjin Xian, “Lossless embedding: A visually meaningful image encryption algorithm based on hyperchaos and compressive sensing,” Chinese Physics B, Volume 32, No. 2, 2023, 020503.

[24] Tutuncu K. and Demirci B., “Adaptive LSB Steganography on Chaos Theory and Random Distortion,” Advances in Electrical and Computer Engineering, volume 18, Issue 3, 2018, pp. 15-22.

[25] D. Molato, F. B. Calanda, A. M. Sison and R. P. Medina, "LSB-based Random Embedding Image Steganography Technique Using Modified Collatz Conjecture," *2022 7th International Conference on Signal and Image Processing (ICSIP)*, Suzhou, China, 2022, pp. 367-371.

[26] Shahidrahman, Jamal Uddin, Hameed Hussain et al. A Huffman Code LSB based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of an image, 08 March 2023, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-2579014/v1]

[27] Rana S. Hameed, Siti S. Mokri, Mustafa S. Taha and Mustafa M. Yaher, “High Capacity Image Steganography System based on Multi-layer Security and LSB Exchanging Method,” International Journal of Advanced Computer Science and Applications(IJACSA), 13(8), 2022.

[28] Sama N. M. Al-Faydi, Shar Khalid Ahmed and Heba N. Y. Al-Talb, “Improved LSB image steganography with high imperceptibility based on cover-stego matching,” IET Image Processing, volume 17, Issue 7, 29 May 2023, pp. 2072-2082.

[29] Hsien-Wen Tseng and Hui-Shih Leng, “A reversible modified least significant bit matching revisited method,” Signal Processing: Image Communication, volume 101, February 2022, 116556.

[30] Ambika, Virupakshappa and Sachinkumar Veerashetty, “Secure communication over wirless sensor network using image steganography with generative adversarial networks,” Measurement: Sensors, volume 24, December 2022, 100452.

[31] Krystian Grzesiak, Zbigniew Piotrowski and Jan M. Kelner, “A wireless covert channel based on dirty constellation with phase drift,” Electronics, volume 10, 2012, 647.

[32] Asmaa A. Eyssa, Fathi E. Abdelsamie and Abdelaziz E. Adelnaiem, “An efficient image steganography approach over wireless

communication system," Wireless Personal Communication, volume 110, 2020, pp. 321-337.

[33] Lin, Hanhe and Hosu, Vlad and Saupe, Dietmar, "KADID-10k: A Large-scale Artificially Distorted IQA Database," In Proceeding of 10th International Conference on Quality of Multimedia Experience (QoMEX), IEEE, 2019, pp. 1-3.

[34] T.S. Rappaport, Wireless Communications, Prentice-Hall, 1996.

[35] Hacimurtazaoglu M, Tutuncu K. 2022. LSB-based pre-embedding video steganography with rotating & shifting poly-pattern block matrix. Peer J Comput. Sci. 8:e843.

[36] Amirfarhad Nilizadeh, Shirin Nilizadeh, Wojciech Mazurczyk, Cliff Zou and Gary T. Leavens, "Adaptive Matrix Pattern Steganography," Journal of Cyber Security and Mobility, Vol. 11(1), pp. 1–28, 2021.

[37] Huang, C.T.; Shongwe, N.S.; Weng, C.-Y. Enhanced Embedding Capacity for Data Hiding Approach Based on Pixel Value Differencing and Pixel Shifting Technology. Electronics 2023, 12, 1200.

[38] Granados, C. (2023). Convergence of Neutrosophic Random Variables. Advances in the Theory of Nonlinear Analysis and Its Applications, 7(1), 178–188.

[39] Naas, A., Benbachir, M., Abdo, M. S., & Boutiara, A. (2022). Analysis of a fractional boundary value problem involving Riesz-Caputo fractional derivative. Advances in the Theory of Nonlinear Analysis and Its Applications, 6(1), 14–27.

[40] Khetani, V., Gandhi, Y., Bhattacharya, S., Ajani, S. N., & Limkar, S. (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253-262.

[41] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825