[1] Mukund D. Maid

[2] Pratik R. Hajare

Patch-based Reversible Steganography for Secured Communication over Wireless Channels

Abstract: - Securing the perceptual quality of the cover image (CI) and acquiring higher security for hidden information in stego images (STIs) are two sides of the same coin. There is always a trade-off between perceptual quality and level of security when secret bits (SBs) of the secret image (SI) are embedded in a CI. Non-reversible techniques are adopted where a higher level of security is required as in communication, while reversible schemes are preferred to maintain the visual quality of the CI. This article proposes a novel Patch-Based LSB Embedding (LSBE) Data Hiding (PB-LSB-EDH) scheme that provides better security to SBs and maintains stego quality. The scheme embeds a secret byte in a 3x3 patch of the CI. The starting byte in the neighborhood where the SBs are hidden is computed from the center pixels of the 3x3 patch window and continues to embed pixels clockwise. The PB-LSB-DH scheme is highly immune to external noise or attacks when the intensity value of the center pixels is equal to or greater than 12 since the starting index of bit embedding is computed using a natural logarithm. Experimental analysis of four different CIs and SIs showed that the proposed PB-LSB-DH scheme maintains the better perceptual quality of the CI and a higher peak signal-to-noise ratio (PSNR) above 50.

Keywords: *CI, stego images, SI, Non-reversible techniques, Patch-Based LSBE Data Hiding (PB-LSB-EDH) scheme, natural logarithm, and peak signal-to-noise ratio.*

1. Introduction

Secret information is concealed in such a way that the SBs are imperceptible within a covered object or entity. The secret data is hidden using an image, audio signal, text, or video. The challenge in steganography is to cover useful information intelligently with minimal distortion or contamination of the CI. Another important aspect of steganography is to devise an efficient mathematical or statistical approach for extracting the SBs reversibly causing no distortions and alignments. The basis of modern approaches is governed by accurate and consistent data independent of sophisticated complex analytical frameworks. Such application frameworks incorporating the latest steganography schemes can be referred from [1-9]. Rapid advancements involving different principles and techniques can be seen in [10-20] related to steganography. Work seen in the literature is focused on either data redundancy exploitation for maximizing the capacity or reversible message encoding.

Steganography algorithms using the spatial domain approach are simpler and require minimum computations. They use the least significant bit (LSB) of the CI to hide the secret or a sensitive bit of the SI. The data-hiding strategy does not deteriorate the CI or degrade the imperceptibility of the CI. The channel impact of a single secret bit in the LSB of the covering byte is minimal and can be resolved using a simpler steganalysis algorithm while recovering the hidden bit. However, such spatial domain-based approaches used for data hiding are susceptible to unseen attacks. Methods like LSBE, random embedding, histogram shifts, intensity-based, index labelling, etc. are some of the simple approaches used for steganography using the spatial domain. On the other hand, transform-based approaches make use of transform coefficients to hide the secret information. The original pixel values are transformed into new values for hiding the information. Most of the methods usually are non-reversible but provide better robustness towards vulnerable attacks. The pixel intensity values are converted using methods like wavelets, stationary wavelets, discrete trigonometric transforms, or other transformations that can change values for the parent pixel of signal values.

Some of the expected performance parameters to measure the performance of a quality steganography approach are worked out by Hussain and Hussain [21]. The expectations include perceptual transparency, resistance offered,

[1] PhD Scholar, Mansarovar Global University, Bhopal, Madhya Pradesh.

[2] Professor, Mansarovar Global University, Bhopal, Madhya Pradesh

substantiality, complexity, and capacity. The next section includes some of the state-of-the-art steganography techniques by researchers.

2. Related Work

The most commonly used technique for hiding secret data in the CI is the LSBE scheme which is improved in most of the articles in one way or the other. The simplest scheme offers low complexity and a simpler approach at the cost of insecurity which allows any intruder to extract the secret information easily. The authors in [22] used a pseudo-random LSBE scheme and produced the STI with the help of indexes. However, their scheme offered poor resistance to attacks and required a robust pseudo-random generator. Higher security with better imperceptibility of the CI was the work carried out in [23-26] for JPEG images. The secret data was rearranged using a Genetic Algorithm (GA) which was used to search for best-tuned parameters for the Logistic Map before hiding into the CI. They adopted a chaotic random number generator and a GA in conjunction for obtaining the STI. Work focused on variable steganography was introduced in [27-29]. They used a single 2D chaotic map and a mixed approach combining matrix encoding and LSB encoding using a cross-coupled chaotic map for specifying the coordinates of different segments of the hidden details. Improved performance concerning fidelity and imperceptibility was seen in [30] and [31] using a 3D chaotic map with wavelet transform (WT) and integer WT respectively. The schemes also obtained higher PSNR along with superior fidelity and good imperceptibility.

AES (Advanced Encryption Standard) algorithm and integer WT were introduced in [32] for embedding the SBs. The authors divided the host image into fixed-size blocks for LSBE and suffered perceptible distortion for higher data capacity. A two-stage embedding scheme was introduced to provide better security and was achieved using scrambling and encryption in most of the cases. The embedding information was limited using only edge details in the case of [33]. Edges were determined using a filter and DCT (Discrete Cosine Transform) was applied to individual color components of the RGB image. The authors computed half difference and half mean of R & B channels and embedded the binary represented R and B channel information in the G color component coefficients equally. Their method suffered from data deformation due to noise introduced in the edge information uplifted the edges. The work in [34] used scrambling in HSV color space for low-capacity embedding. The secret information was encrypted using an iterative magic matrix encryption method. Other such methods for low-capacity steganography were introduced in [35-36]. They used quantized DCT with 2-dimensional Haar Discrete WT on Y-CbCr color frames respectively. The authors in [37] introduced a high-capacity data embedding scheme and embedded all three color components using DWT. They decomposed the secret and the CIs into 4 bands and then embedded the approximation coefficients of the SIs in CI color planes.

Our Contributions

The article contributes in the following ways concerning steganography:

1. The work introduces a simple and efficient reversible data hiding scheme with low computational complexity,

2. The natural logarithmic value of the magnitude of the center pixel (CP) is used to find the starting index for hiding the SBs (MSB first) in the 8-pixel neighborhood exploiting the use of any randomization approach.

3. The scheme is highly immune to noise since only one pixel (central pixel) is significant in determining the initial position of the clockwise embedding in the 3x3 patch neighborhood.

4. The scheme not only provides higher security, and good imperceptibility but also a higher PSNR value.

Method and Materials

The proposed PB-LSB-EDH scheme initially uses preprocessing of the CI and the SI by adjusting their sizes so that the SI can be secretly hidden in the CI. The height (Rsize) and the width (Csize) of the CI are reduced to a multiple of patch dimension since a patch of 3x3 is considered to hide a byte from the SI. This is achieved by eliminating extreme rows and columns as required from the original CIs. The SI is then resized to dimensions height/3 and width/3 using bicubic interpolation so that all the bytes in the SI can be accommodated in the CI. The secret and the CIs are used from distinct datasets (BDD100K, LabelMe, KITTI, and Places365).

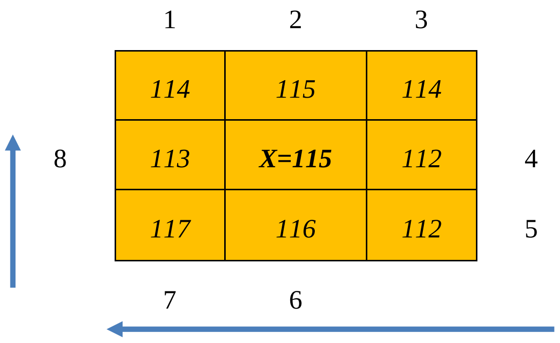
The Data Hiding Mechanism

The following Figure 1 shows how the SBs from a secret byte (SB) in the SI are embedded in a 3x3 patch of the CI. The CP of the 3x3 patch from the CI shown has an intensity value of X=115. The 8-neighbors surrounding the CP as indexed from 1 to 8 in the figure have intensity values 114, 115, 114, 112, 112, 116, 117, and 113 in the clockwise direction. The requirement is to search the starting position in the neighborhood from where the LSBE of SBs would start in the clockwise direction. The initial or the starting index is computed using the following expression (1) which takes into account the value of X.

$$\text{Index } (I) \;= \text{round}\left(\frac{\log CPv}{\log 2}\right) \qquad (1)$$

Where, '*I*' is the starting index from neighboring byte indexes 1 to 8 as shown in the figure, and '*CPv*' is the value of the CP. The 'log' in the expression (1) corresponds to the Natural Logarithm. Thus, for *X=115*, the value of *I* evaluates to 7. It means that the first bit of the secret byte (MSB first –D7 bit) will occupy position in the byte placed at index 7 (value 117) in the neighborhood of the CP. The remaining SBs from D6 to D0 of the secret byte are sequentially embedded in neighboring bytes at index 8, 1, 2, 3, 4, 5, and 6 respectively in a clockwise fashion.

The direction of the arrow marked in Figure 1 indicates the clockwise direction of the SBs embedding process once the initial starting index for the first bit is computed using expression (1).



114	*115*	*114*
113	***X=115***	*112*
117	*116*	*112*

Figure 1 – 3x3 block from the CI

It means that for every such secret byte and every cover 3x3 patch, the initial index is function of the magnitude of the CP. Due to the rounding operation in expression (1), the index for *CPv* = 0, 1, and 2, the embedding starts from the top left corner byte (value 114). Also, for *CPv* = 3, 4, and 5 the value of the initial index *I* is 2, therefore the embedding will start from the top middle byte (115). For *CPv* values ranging from 6 to 11, *I* = 3 (top right byte with value 114). Thus, the offset is minimal when the CP value ranges from 0 to 2, 3 to 5, and 6 to 11.

Any unwanted distortion during transmitting such information over the communication channel may mislead the receiver. A small positive shift may ruin the indexing sequence and the recovered secret byte would differ from actual transmitted information. Table 1 below shows the available offset for all indexes as per the intensity of the CP.

Table 1 – Initial MSB position of SB, Offset as function of *CPv*.

Cpv / index	1 (MSB)	2	3	4	5	6	7	8 (LSB)	Available Offset
0-2	1	2	3	4	5	6	7	8	3
3-5	8	1	2	3	4	5	6	7	3
6-11	7	8	1	2	3	4	5	6	5
12-22	6	7	8	1	2	3	4	5	11
23-45	5	6	7	8	1	2	3	4	23

46-90	4	5	6	7	8	1	2	3	45
91-181	3	4	5	6	7	8	1	2	91
182-255	2	3	4	5	6	7	8	1	74

It is seen from Table 1, that as the magnitude of the CP increases beyond 12, the chances of a positive shift due to channel noise or unseen attacks will not affect the computational value of the starting index I. However, it will have a severe effect when the value of CPs falls in the range of 0 to 12. Even a small drift in value of the CP would shift the starting index below value 12 and the transmitted byte will not be recovered at the receiver accurately. To compensate output of the natural logarithm for CP = 0 and 1, we use the following expression (2) since for CP=0, *I* becomes infinity (*NaN*), and for CP = 1, the value of I will be evaluated to 0.

$$\mathrm{I} = \begin{cases} 1 & CPv == 0 \\ 1 & CPv == 1 \\ \mathrm{round}\left(\frac{\log CPv}{\log 2}\right) & otherwise \end{cases} \qquad (2)$$

Once the starting index is found using expressions (1) and (2), the secret byte is binarized and bits are extracted to embed. The neighboring bytes of the CI are also binarized in sequence depending on the initial index in the clockwise direction. The SBs are then hidden in the LSB position of the neighboring bytes of the CI. Each time a 3x3 patch from the CI and bytes from the SI are considered in a book-reading fashion and the process of LSBE is performed to finally obtain the STI.

The important aspect of the proposed PB-LSB-EDH scheme is that the value of the CP is unaffected during the process of embedding. This ensures greater imperceptibility if 50% of LSB is considered to change in the neighboring bytes of a patch. The STI will certainly maintain the resemblance of the CI and using a 50% replacement in LSB of 8 neighboring bytes, the PSNR will be more than 50 (due to the unaffected value of the CP). The flowchart of the PB-LSB-EDH scheme is depicted in Figure 2. It shows only the embedding process of the secret byte in a 3x3 patch of the CI.

The scheme has low computational complexity since it includes a division operation over logarithmic values followed by a rounding operation. It consumes time when the neighboring bytes are converted from decimal to binary and after secret bit embedding back to decimal.

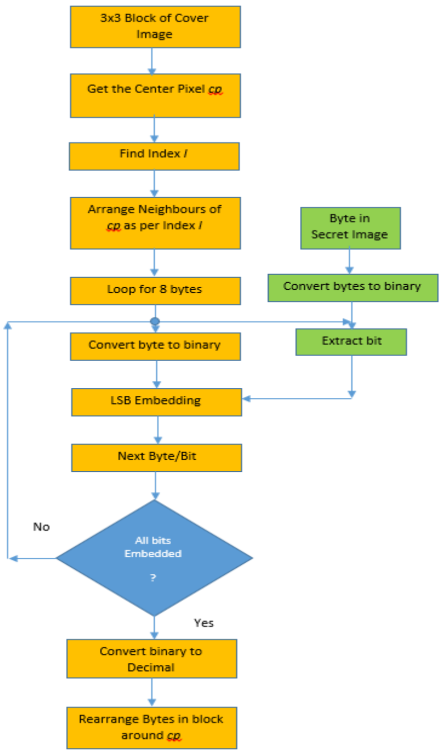


Figure 2 – The framework of PB-LSB-EDH scheme

3. Results and Conclusion

The proposed data embedding scheme was executed on MATLAB 2021b with 512 SSD, 16 GB working memory, i5 INTEL, 2.70 Gigahertz processor, and Windows 11 platform. Experimental analysis using images from BDD100K, LabelMe, KITTI, and Places365 datasets showed that the PB-LSB-EDH scheme obtained higher PSNR values concerning other state-of-the-art methods found in the literature. Figures 3, 5, 7, 9, and 11 show the CIs, SIs, and STIs obtained using the proposed secret data embedding scheme. The perceptual quality of the STIs is better and shows a nearer resemblance with the CIs. The effect of hiding the SI is negligible as far as the deterioration of the original CI is concerned. Even the homogeneous regions in the CIs do not show any degradation due to secret data. Thus, the proposed PB-LSB-EDH scheme ensures the secrecy of the information in the CI. Figures 4, 6, 8, 10, and 12 show the original SI, the STI, and the recovered SI after reversing the LSB hiding scheme.

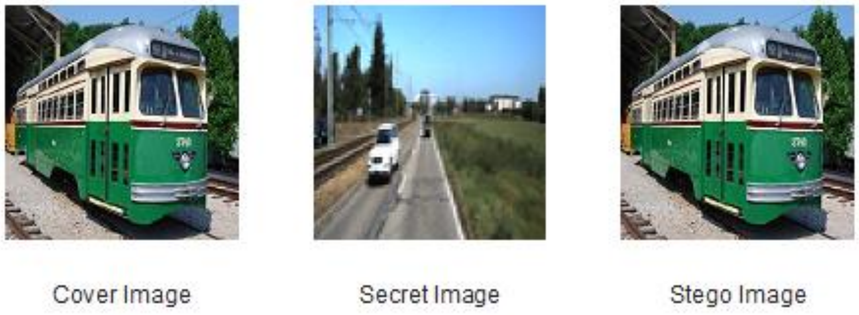


Figure 3 – CI from Places365, SI from KITTI, and generated STI.

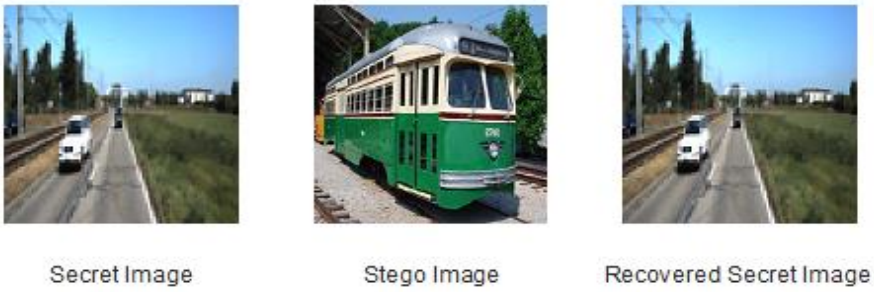


Figure 4 – The SI, STI, and the recovered SI for CI in Figure 3.

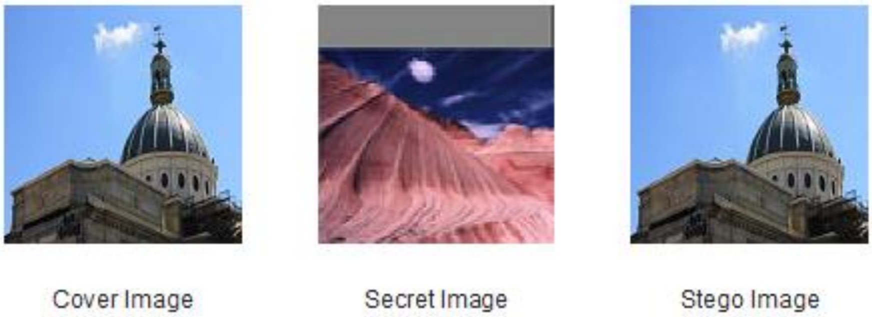


Figure 5 – CI from Places365, SI from BDD100K, and generated STI.

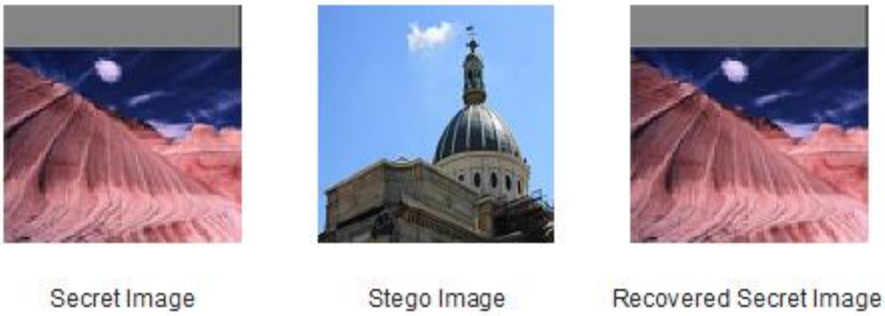


Figure 6 – The SI, STI, and the recovered SI for CI in Figure 5.

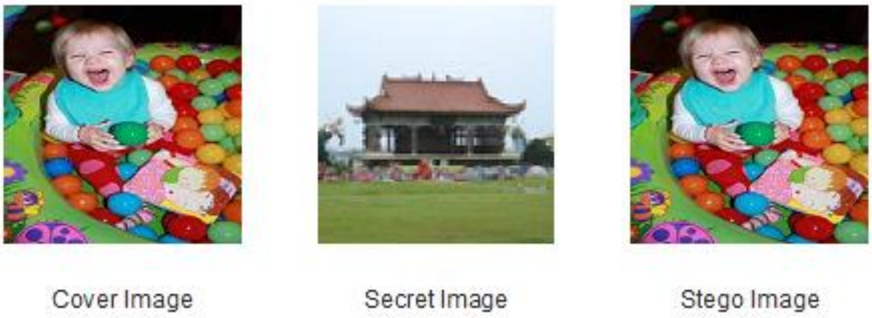


Figure 7 – CI from Places365, SI from LabelMe, and generated STI.

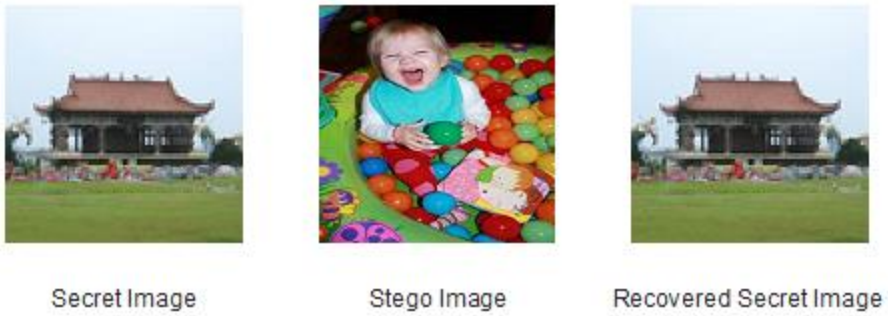


Figure 8 – The SI, STI, and the recovered SI for CI in Figure 7.

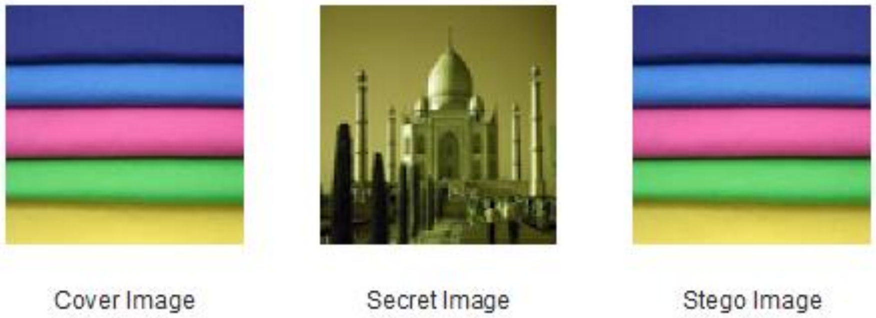


Figure 9 – CI and SI from Places365, and generated STI.

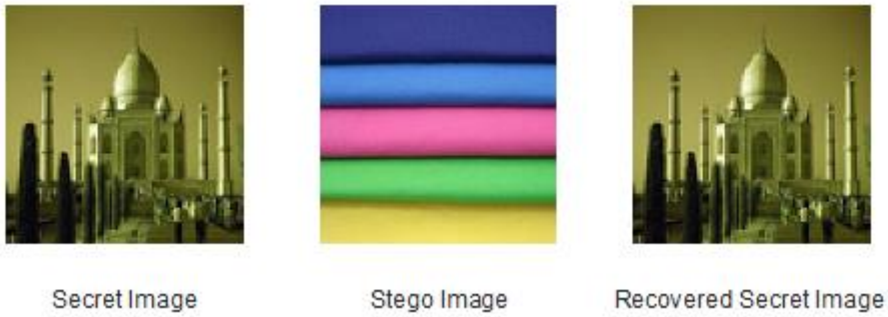


Figure 10 – The SI, STI, and the recovered SI for CI in Figure 9.

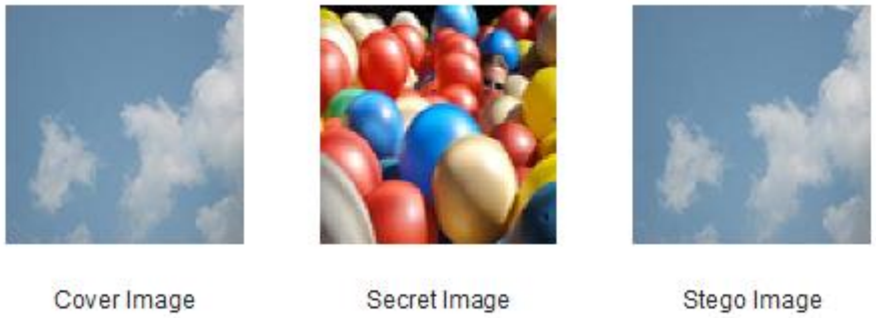
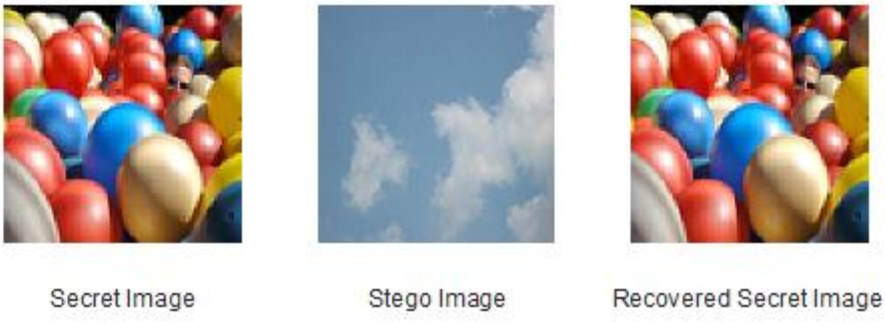


Figure 11 – CI and SI from Places365, and generated STI.



Secret Image Stego Image Recovered Secret Image

Figure 12 – The SI, STI, and the recovered SI for CI in Figure 11.

We chose five different CIs and SIs from the datasets and evaluated the performance of our scheme with respect to PSNR. Table 2 lists the PSNR measure for different image combinations. The PSNR values for all the combinations are well above 51 even if SIs with saturated color are used over faint CIs. The PB-LSB-EDH scheme iterates for RGB color components of the images. Each color component of the SI is hidden in the respective color frames of the CI. The scheme provides a high level of security and greater imperceptibility at the cost of a data capacity of 9:1. A small change in the low value and a drastic change in higher values of the CP may affect the scheme's performance. The former has a higher probability in the case of Additive White Gaussian Noise (AWGN) when information is transmitted over a wireless communication system. However, the latter has a minimal probability of occurrence. Thus the performance of the proposed PB-LSB-EDH scheme can be evaluated over AWGN channel for Wireless Communication System.

Table 2 – PSNR for combinations of CIs and SIs from four datasets as considered in figures 3 to 10

Cover/SI	KITTI	BDD100K	LabelMe	Places365	Places365
Places365	51.6324	51.6437	51.6348	51.3245	51.6488
Places365	51.6561	51.6803	51.6618	51.6606	51.6309
Places365	51.6314	51.6930	51.6440	51.6802	51.6525
Places365	51.6553	51.6534	51.6554	51.6477	51.6737
Places365	51.6591	51.6669	51.6646	51.6339	51.6702

References

[1] 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.

[2] I. 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] A. 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] M. Hussain and M. Hussain, "A survey of image steganography techniques," 2013.

[22] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," IEE Proceedings - Vision, Image and Signal Processing, vol. 147, no. 3, pp. 288-294, Jun. 2000. doi:10.1049/ip-vis:20000341

[23] W. Wong, L. Lee, and K. Wong, "A Modified Chaotic Cryptographic Method," in Communications and Multimedia Security Issues of the New Century: IFIP TC6 / TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01) May 21-22, 2001, Darmstadt, Germany, R. Steinmetz, J. Dittman, and M. Steinebach, Eds. Boston, MA: Springer US, 2001, pp. 123-126. doi:10.1007/978-0-387-35413-2_11

[24] A. Kanso and N. Smaoui, "Irregularly decimated chaotic map (s) for binary digits generations," Internatio Chaos, vol. 19, no. 04, pp. 1169-1183, 2009. doi:10.1142/S0218127409023573

[25] A. Kanso, H. Yahyaoui, and M. Almulla, "Keyed hashed function based on a chaotic map," Information Sciences, vol. 186, no. 1, pp. 249-264, 2012. doi:10.1016/j.ins.2011.09.008

[26] A. Kanso, "Self-shrinking chaotic stream in nonlinear science and numerical simulation, vol. 16, no. 2, pp. 822-836, 2011. doi:10.1016/j.cnsns.2010.04.039

[27] A. Kanso and H. S. Own, "Steganographic algorithm based on a chaotic map," Communications in Nonlinear Simulation, vol. 17, no. 8, pp. 3287-3302, Aug. 2012. doi:10.1016/j.cnsns.2011.12.012

[28] R. Roy, A. Sarkar, and S. Changder, "Chaos-based Edge Adaptive Image Steganography," Procedia Technology, vol. 10, pp. 138-146, Jan. 2013. doi:10.1016/j.protcy.2013.12.346

[29] S. Ahadpour and M. Majidpo Discrete Cross-Coupled Chaotic Maps," 2013.

[30] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography," Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 6, pp. 1898-1907, J doi:10.1016/j.cnsns.2013.10.014

[31] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic c color images," Journal of Information Security and Applications, vol. 34, pp. 142-151, Jun. 2017. doi:10.1016/j.jisa.2017.04.004

[32] Seethalakshmi, K. S., Usha, B. A., & Sangeetha, K. N. (2016). Security enhancement in image steganography using neural networks and visual cryptography. In 2016 International Conference on Computation System

and Information Technology for Sustainable Solutions (CSITSS), IEEE conference publications (pp. 396–403).

[33] Lahiri, S., Paul, P., Banerjee, S., Mitra, S., Mukhopadhyay, A., & Gangopadhyaya, M. (2016). Image steganography on colored images using edge-based Data Hiding in DCT domain. In 2016 IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON) (pp. 1–8).

[34] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., & Baik, S. W. (2016). Image steganography using uncorrelated color space and its application for the security of visual contents in online social networks. Future Generation Computer Systems (in press, Corrected Proof, Available online 27 November 2016).

[35] El Rahman, S. A. (2016). A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors' confidential information. Computers and Electrical Engineering (Available online 19 September 2016).

[36] Broda, M., Hajduk, V., & Levický, D. (2015). Image steganography based on a combination of the YCb-Cr color model and DWT. In 2015 57th international symposium ELMAR (ELMAR), Zadar (pp. 201–204).

[37] Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT-based image securing method using steganography. In International conference on information and communication technologies (ICICT 2014).