ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

Image Steganography Using Center Pixel Offset Based LSB Embedding Scheme

Abhijit S. Mali[1*] and Manoj M. Dongre[2]

[1.2]Department of Electronics and Telecommunication, 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

How to Cite: **Abhijit S. Malia and Manoj M. Dongre. (2024), Image Steganography Using Center Pixel Offset Based LSB Embedding Scheme, International Journal of Applied Engineering Research, International Journal of Applied Engineering & Technology 5(4), pp.1130-1137.**

Abstract **- When it comes to perceptual quality and security, steganography has been a key topic. The perceived quality of the stego image is reduced when high security is obtained; hence there is a trade-off between these two characteristics. With a very small computational cost, the Center Pixel offset 'X' Based LSB Embedding technique suggested in this study is able to maintain both metrics. The pseudo random and chaotic LSB embedding system is a comparable scheme that improves stego quality while also improving secret message security. The location in the 3x3 neighbourhood from where the LSB embedding would commence is determined using the centre pixel value and offset value. Natural logarithm with offset applied to the magnitude of the centre pixel yields a straightforward formula for calculating the index in the neighbourhood. The embedding process moves clockwise around the neighbourhood. The band widens after value 12 and no amount of attack or noise will be able to push the value outside of the band, making the suggested approach extremely resistant to unintentional noise or attack in stego photos at centre pixel values higher than or equal to 12. The maximum signal to noise ratio and stego picture perception quality is used to gauge the effectiveness of the system using four cover photos and four concealed images.**

Index Terms **- Center Pixel, Image Steganography, LSB embedding, stego image.**

INTRODUCTION

Steganography is the process of hiding hidden information inside a covered object or creature such that it cannot be seen. You can use a voice, image, text, or video as a cover for concealed data. Since significant information must be integrated with intelligence while minimizing distortion and contamination in the cover item, modern steganography is challenging in the scientific arts. Creating a steganography system that allows the mathematical technique to extract the secret data in a reversible, distortion- and misalignment-free format is another challenge. The cornerstone of modern techniques continues to be reliable and consistent data, regardless of the sophisticated analytical platform being utilised for embedding. [1–9] contains a number of examples of current steganography in use. The field of steganography has quickly advanced thanks to a range of concepts and methods for reversible steganography [10–20]. The focus of the literature is either on using data redundancy to boost data capacity or on encrypting a message in a reversible, undetectable way. The two primary categories of algorithms utilized in picture steganography are transform domain techniques and spatial domain strategies. Due to their low computational requirements and simplicity, spatial domain approaches like luminance-based, LSB embedding, arbitrary embedding, etc., are often utilised. Typically, the least significant bit is used in spatial approaches to hide important or secret elements of the underlying picture. From a perceptual standpoint, the cover image experiences less degeneration and does not suffer significantly. Any of the known steganalysis techniques can be used to solve a single embedded bit's channel impact, which is minimal, to recover the lost bit. The bulk of these strategies may be attacked because of how straightforward they are. Transform-based algorithms, on the other hand, conceal the secret data that was obtained through a transform, such as a wavelet, a discrete fourier, a discrete cosine, a stationary wavelet, or any other transformation that can generate new values in relation to the distinct pixel intensities and can be recreated with little artefact. They also provide a stronger defence against ineffectual attacks because of their strength. Expectations for effective steganography are covered in [21] by Hussain & Hussain and include things like capacity, aesthetic transparency, computational difficulty, inherent resistance, and substantiality. The following section provides a summary of some of the study data that has been offered as support for image steganography.

RELATED WORK

Improvements to LSB embedding schemes have yielded significant results in most of the literatures, but at the expense of security due to the ease with which hidden information can be discovered. The technique suggested in [22] employed pseudo random LSB embedding and produced stego images using indexes, however these methods give only little protection against any unforeseen assault, necessitating the employment of a robust pseudo random generator. The perceived picture quality was preserved while achieving high capacity and security. In order to provide coordinates of different concealed message components, the approach described in [27–29] combines matrix encryption with LSB embedding, variable-sized steganography that uses a single 2-D chaotic map, and cross-coupled chaotic maps. New techniques were developed with the promise of improved fidelity and good imperceptibility at greater PSNR. Among these techniques were the unexpected map with integer wavelet transform [31], the 3-D chaotic maps with lifted wavelet transform [30], and others.

Scrambling, encryption, and two-stage security methods have all been incorporated in recent security research. In [32], after the host image was separated into blocks for LSB embedding, the secret data was injected using the Advanced Encryption Standard algorithm and integer wavelet transform.

After the host image was separated into blocks for LSB embedding, the secret data was injected using the Advanced Encryption Standard algorithm and integer wavelet transform.

As the data volume expanded, the approach underwent a significant distortion. By utilising a filter to identify the edges in the colour image and then applying Discrete Cosine transform to each individual colour channel, data size was constrained in [33]. The GREEN channel was then evenly embedded with the calculated coefficients. Then, the RED and BLUE channels' half differences and half averages—represented by 0 and 1—were determined. When the noise grew in edge positions, the system showed signs of data distortion. The secret data was encrypted using an iterative magic matrix encrypting algorithm and fragmented data in the HSV colour space, using a low-capacity model from [34]. They were able to create high-quality stego images with this technique while utilising very little storage by simply employing the V plane for embedding with LSB. As comparable techniques for low-capacity steganography, the quantized discrete cosine transform and the 2D Haar Discrete Wavelet transform on YCbCr components were used in [35] and [36], respectively. [37] increased data capacity by embedding three hidden images into RGB colour planes using the discrete wavelet approach. Using a discrete wavelet transform, the cover picture and the hidden photos were divided into four bands, with the approximate band of the hidden photos being added into each of the external image's colour planes.

CONTRIBUTION

For steganography, this technique suggested using a centre pixel offset-based LSB embedding scheme. The secret bits are inserted in the cover image block bytes, which is where the innovation is found. In this example, the believability or magnitude of the central pixel is utilised to choose which byte in the 3x3 district the initial hidden bit should be placed from, as opposed to employing a random or disordered distribution to hide useful bits. All subsequent bits are then positioned in the LSB position of succeeding bytes after the first bit in the hidden information is placed in the MSB position (MSB first) in the centre pixel.

IMPLEMENTED METHODOLOGY

The dimensions of the cover up image and the top-secret picture are changed in the proposed work such that a byte from the secret image can be embedded for every 3x3 block from the cover image. By removing the excessive row/rows and column/column sizes, the cover image's row and column sizes [rsize, csize] are scaled to multiples of 3. The secret image is then downsized using bilinear interpolation to a element where its row and column sizes are [rsize/3, csize/3]. In order to assess the effectiveness of the suggested technique, the cover photos and the hidden images are taken from two different datasets.

Here, a 3x3 chunk in the cover image, as illustrated in figure 1 below, is taken into consideration:

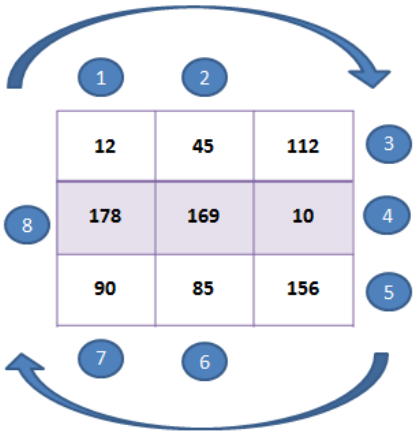

FIGURE 1. 3 × 3 BUILDING BLOCK FROM THE COVER IMAGE

Let's assume that the secret image's byte needs to be 100 in order for it to be included in this block. Note that the central pixel in Figure 1 has a value of 169. Finding the byte in the block that includes the first bit of the confidential data is the goal. (First the MSB of the hidden image). The bytes in the area of 169 are numbered sequentially, as seen in figure 1. The first byte (12) is in the upper left corner, and the next bytes are labelled from left to right, downward to below, and then upward. Thus, the number 8 is assigned to the last byte (178). The initial neighbor numbering from which the embedding would begin is indicated by the arrow in figure 1. Determine the beginning point with relation to the pixel's center's magnitude and added encrypted offset value X (0 to 7). The following equation 1 is used to evaluate the starting point.:

$$\text{Index (I)} = \text{round}\left(\frac{\log cp}{\log 2}\right) + \text{X} \quad (1)$$

Here 'X' is the encrypted integer offset value added in the I, where I denotes the initial position from which the first bit of the secret image should actually be embedded and is represented by a number. The value of the center pixel is denoted by the symbol cp, and the expression's "log" stands for the natural logarithm. Figure 1's arrow shows that the embedding process moves in a clockwise direction. The only distinction would be in the numbering, which would depend on the value of the expression 1. The formula 1 was modified in this manner to take into consideration the values of cp = 0 (infinity) and cp = 1 (zero).:

$$I = \begin{cases} 1 + X & cp == 0 \\ 1 + X & cp == 1 \\ round\left(\frac{\log cp}{\log 2}\right) + X & otherwise \end{cases} \quad (2)$$

Additionally, we rounded the result of logcp/log2 to the nearest integer value. As a result, for cp = 0, 1, and 2, the embedding will begin at the block's top left corner, if X=0 (byte 12) and work its way down in the direction of the arrows. Index I will be 2+X for cp = 3, 4, and 5. Block 2+X will provide the starting position, followed by the arrow direction, and byte 156 will contain the final bit. i. e. 2+3(for X=3), which is initially designated as 5. The embedding would begin at byte 156 in the bottom right corner (formerly numbered 5), and byte 10 (originally numbered as 4) would take up the final bit of the secret picture for cp = 6 to 11. The change in index in relation to the size of the center pixel and X=3 is displayed in Table 1 below. Figure 2 depicts the flowchart for the center pixel offset based LSB embedding system that has been proposed for steganography.

TABLE 1. FOR X=3, THE MODIFIED INDEX WITH REGARD TO THE VALUE OF THE CENTER PIXEL, "CP,"

Initial index	1 (MSB)	2	3	4	5	6	7	8 (LSB)
0-2	7	8	1	2	3	4	5	6
3-5	6	7	8	1	2	3	4	5
6-11	5	6	7	8	1	2	3	4
12-22	4	5	6	7	8	1	2	3
23-45	3	4	5	6	7	8	1	2
46-90	2	3	4	5	6	7	8	1
91-181	1	2	3	4	5	6	7	8
182-255	8	1	2	3	4	5	6	7

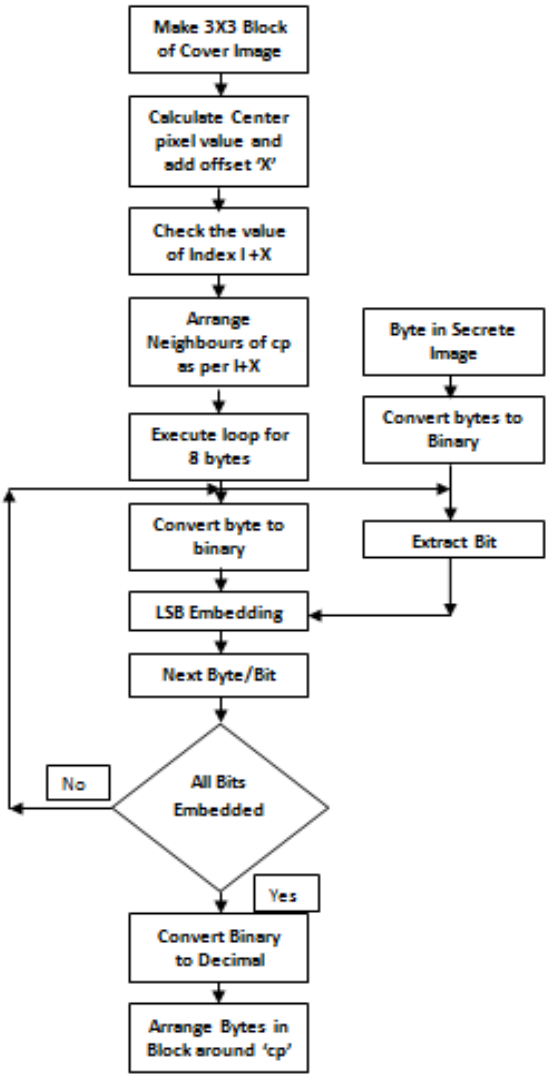

FIGURE 2: DESIGN FLOW

The secret byte from the secret picture and the surrounding bytes in the cover image are converted to binary once expression 2 has taught us the starting byte of the cover image. After that, an iterative LSB embedding from MSB to LSB process is applied to each of the first eight bytes. After that, based on the block location that corresponds to the covering picture, all eight of the neighboring bytes are converted to binary and replaced in the stego image. By keeping the value of the central pixel in the stego image constant, the technique used here maintains the apparent quality of the final stego image in proportion to the cover image. Considering that the peak signal to noise ratio is greater than 50 while maintaining the higher perceptual quality of the stego picture, the low-frequency band (LSB) in the cover image is probably equal to or greater than 50% of the LSB in the secret byte.

RESULTS

In this approach, four cover images and four secret photographs were selected from two separate datasets, and the effectiveness of the job was assessed using MATLAB 2021b and an i5, 2.70 GHz processor with 16 GB of RAM. In order to calculate the peak signal to ratio, all hidden images and cover photos were used in the study. Table 2 illustrates the efficacy of the center pixel offset based LSB embedding technique. There is higher perceptual quality across all 16 PSNR values, all of which are more than 50. Though it takes less time and processing power, the task is equivalent to randomized LSB embedding. Figures 3 and 4 displays the outcomes of cover image 1 and secret image 1. When compared to the original cover image, Figure 3 shows how the stego image has a higher perceptual quality. Figure 4 shows how the hidden picture was successfully extracted from the stego image when the PSNR was infinite. Figures 5, 6, and 7 display the corresponding generated stego images for the same cover images 2, 3, and 4 for the hidden image 1. The cover photographs are chosen to include a portion of the sky and objects with rich colors so that the deterioration of the hidden image may be seen clearly after embedding. The resulting stego images show that the proposed embedding strategy has not significantly degraded. Instead of being compared to other state-of-the-art studies from other literatures, the PSNR is used to evaluate the efficacy of the center pixel offset based approach.

FIGURE 3. STEGO IMAGE FOR COVER IMAGE 1 GENERATED

FIGURE 4. RECOVERED SECRET IMAGE

FIGURE 5. STEGO IMAGE FOR 2NDCOVER IMAGE

FIGURE 6. STEGO IMAGE FOR 3RD COVER IMAGE

FIGURE 7. STEGO IMAGE FOR COVER IMAGE 4

FIGURE 8. IN THIS PIECE, SECRET IMAGES 2, 3, AND 4 WERE UTILIZED

TABLE 2 – PSNR VALUES FOR VARIOUS SECRET AND COVER IMAGES

Cover/Secret Image	Secret Image 1 (Tomato)	Secret Image 2 (Clock)	Secret Image 3 (Pencil)	Secret Image 4 (Parrot)
Cover Image 1 (Cow)	51.5484	51.6784	51.6127	51.6360
Cover Image 1 (Dog)	51.6111	51.6847	51.6246	51.6683
Cover Image 1 (Elephant)	51.6383	51.5535	51.5520	51.6342
Cover Image 1 (Sunflower)	51.5475	51.6340	51.6181	51.6632

CONCLUSION

The proposed center pixel offset based LSB embedding method is resilient in terms of providing high security, but it is computationally easy. It mimics both chaotic and pseudo random LSB embedding approaches. LSB data is embedded differently in each block of the cover picture based on the value of the center pixel and any additional encrypted offset. Every color from the hidden image is represented in the RGB cover image, which also maintains perception quality with a PSNR value over 50. Noise interference in the low range of center pixel values less than 12 may have an impact on the stego image. Since the offset of the center pixel values grows from 11, 23, 45, and so on for bands 12-22, 23-45, 46-90, and so on, values over 12 are unaffected by noise effects. Any meaningful alteration to the center pixel alone could have a substantial impact on the subsequently retrieved hidden image. Once the hidden image is found, there is still an opportunity to recover the affected values from the surrounding area. This approach's tiny embedding capacity (9:1) is its only downside.The work can be improved by implementing appropriate encryption techniques to offer two stage securities. Future work will focus on adding a higher level of security to the embedding mechanism and assessing how well it performs in wireless communication systems that use OFDM over AWGN. (Additive White Gaussian Noise).

REFERENCES

[1] Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G. (1999).: Information hiding-a survey. In: Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078,

[2] Cox, I. J., Kilian, J., Leighton, F. T., Shamoon, T. (1997).: Secure spread spectrum watermarking for multimedia. In: IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687,

[3] Ruizhen, L., Tan, T. (2002).: An SVD-based watermarking scheme for protecting rightful ownership. In: IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128,

[4] Lai, C. C., Tsai, C. C, (2010).: Digital image watermarking using discrete wavelet transform and singular value decomposition. In: IEEE Transactions on Instrumentation and Measurement, vol. 59, no. 11, pp. 3060–3063,

[5] Fridrich, J., Adhikary, M. C. (1998).: Image watermarking for tamper detection. In: Proceedings of International Conference on Image Processing (ICIP), pp. 404–408, Chicago, IL, USA,

[6] Kundur, D., Hatzinakos, D. (1999).: Digital watermarking for telltale tamper proofing and authentication. In: Proceedings of the IEEE, vol. 87, no. 7, pp. 1167–1180,

[7] Lee, T. Y., Lin, S. D. ,(2008).: Dual watermark for image tamper detection and recovery. In: Pattern Recognition, vol. 41, no. 11,pp. 3497–3506

[8] Fridrich, J., Goljan, M., Lisonek, P., Soukal, D. (2005).: Writing on wet paper. In: IEEE Transactions on Signal Processing, vol. 53,no. 10, pp. 3923–3935,

[9] Holub, V., Fridrich, J., Denemark, T. (2014).: Universal distortion function for steganography in an arbitrary domain. EURASIP Journal on Information Security, vol. 2014, no. 1,pp. 1–13,

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

[11] Fridrich, J., Goljan, M. (2001).: Invertible authentication. In: Proceedings of The International Society for Optical Engineering, vol. 4314, pp. 197–208,San Jose, CA, USA,

[12] Vleeschouwer, C. De., Macq, B. (2003).: Circular interpretation of objective transformations in lossless watermarking for media asset management. In: IEEE Transactions on Multimedia, vol. 5, no. 1, pp. 97–105,

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

[14] Alattar, A. M. (2004).: Reversible watermark using the difference expansion of a generalized integer transform. In: IEEE Transactions on Image Processing, vol. 13, no. 8, pp. 1147–1156,

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

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

[17] Huang, X., Nishimura, A., Echizen, I. (2010).: A reversible acoustic steganography for integrity verification. In: Proceedings of International Workshop on Digital Watermarking(IWDW), pp. 305–316, Springer-verlag, Berlin Heidelberg,

[18] Coltuc, D. (2012).: Low distortion transform for reversible water marking. In: IEEE Transactions on Image Processing, vol. 21,no. 1, pp. 412–417,

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

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

[21] Hussain, M., Hussain, M.. (2013).: A survey of image steganography techniques. International Journal of Advanced Science and Technology. Vol. 54, pp. 1-12,

[22] Lee, Y. K., Chen, L. H. (2000).: High capacity image steganographic model. In:IEE Proceedings - Vision, Image and Signal Processing, vol.147, no. 3, pp. 288-294,

[23] Wong, W., Lee, L., Wong, K. (2001). :A Modified Chaotic Cryptographic Method. Computer Physics Communication. Volume-138, pp. 234-236,

[24] Kanso, A., Smaoui, N. (2009).: Irregularly decimated chaotic map (s) for binary digits generations. International Journal of Bifurcation and Chaos, Vol. 19, No. 4, pp. 1169-1183,

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

[26] Kanso, A. (2011).: Self-shrinking chaotic stream ciphers. Common nonlinear sci Numer Simulate. vol. 16, no. 2, pp. 822-836,

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

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

[29] Ahadpour, S., Majidpo, M. (2012).: Public key Steganography using Discrete Cross-Coupled Chaotic Maps. pp. 1-6,

[30] Ghebleh, M., Kanso, A. (2014).: A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 6, pp. 1898-1907,

[31] Valandar, M. Y., Ayubi, P., Barani, M. J. (2017). : A new transform domain steganography based on modified logistic ccolor images. Journal of Information Security and Applications, vol.34, pp. 1-10,

[32] Seethalakshmi, K. S., Usha, B. A., Sangeetha, K. N. (2016).: Security enhancement in image steganography using neural networks and visual cryptography. In : 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.: Image steganography on coloured images using edge based Data Hiding in DCT domain. In : IEEE 7th annual information technology, electronics and mobile communication conference (IEMCON) pp. 1–8, (2016).

[34] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., Baik, S. W. (2016).: Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Generation Computer Systems. pp. 1-10, Elsevier,

[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. pp. 1-20, Elsevier,

[36] Broda, M., Hajduk, V., Levický, D. (2015).: Image steganography based on combination of YCbCr color model and DWT. In : 57th international symposium ELMAR (ELMAR), Zadar Croatia, 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).Procedia Computer Science 46, pp. 612-618,