Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 283–292
DOI : 10.47974/JDMSC-1882

Enhancing digital information concealment through DWT-based coefficient alteration and steganographic technique

Juhi Singh *
Department of Computer Science and Engineering
Manipal University
Jaipur 303007
Rajasthan
India

Arun Kumar Singh †
Department of Electronics and Communication Engineering
Amity University
Gurugram 122413
Haryana
India

Abstract

Concealing information within digital images, blending the realms of art and science, has gained heightened significance in contemporary society. As a substantial amount of personal data is readily available on the world wide web in various formats, including text, still-images, and videos, safeguarding this information becomes imperative. This study explores data hiding through the alteration of coefficients using a DWT. Employing the Data Hiding in the Frequency Domain proves to be more advantageous compared to methods in the other domain. The scaling factor emerges as a pivotal parameter, exerting a substantial influence on key performance metrics. The suggested approach enhances the confidentiality, invisibility, and robustness of concealed data by integrating it within the Discrete Wavelet Transform (DWT) coefficients.

Subject Classification: *Primary 94A08, Secondary 49K15.*

Keywords: *Steganography, Frequency domain, Steganalysis, Gaussian noise, SSIM, Data hiding.*

* *E-mail:* `juhisingh17@gmail.com (Corresponding Author)`
† *E-mail:* `arunsingh86@gmail.com`

1. Introduction

The issues regarding the authenticity of an individual's data as well as issues about the security of data in general have arisen as a direct result of the ease with which data based on text and images may be accessed, used, and shared on the internet. Since the beginning of recorded history, people have been acutely aware of the need to keep the information they exchange private. Consequently, they have devised a broad range of strategies to meet the objective of protecting the privacy of their conversations. The techniques of steganography, by far and away, are the most successful approach internet and to concealing information, preserving the secrecy of data that is transferred while doing so over the internet, and doing so while using the internet [1] [2].

2. Literature Review

Chi Cheng's paper in 2004 explores a straightforward yet effective approach to data hiding within images. The primary focus of the study lies in utilizing the Least Significant Bit (LSB) substitution method, a technique widely recognized for its simplicity and efficiency in concealing information [3]. In Wei Chen's paper published in 2020, the author introduces an innovative approach to data hiding. The focus of the study is on utilizing multi-layer mini-Sudoku techniques for embedding information with high capacity. This method is particularly interesting as it combines the principles of Sudoku puzzles with data hiding, offering a unique perspective on enhancing information concealment [4]. B. Singh's paper, titled published in Multidimensional Systems and Signal Processing in 2020, presents a noteworthy contribution to the field of image steganography. The primary focus of the study revolves around the development of a hybrid algorithm designed to enhance the robustness of image steganography techniques [5]. Patel, Wandra, and Shah's paper introduces a novel approach to image steganography. The authors delve into the intricacies of their proposed algorithm, emphasizing the utilization of pixel swapping and a parity-based technique to conceal information within images [12]. Xie's paper in 2019 explores a novel approach to embedding secret information in multimedia content. The author introduces the concept of an extended squared magic matrix, emphasizing its utility in achieving a substantial payload for information concealment. [9]. Tzu-Chuen Lu's paper published in Signal Processing (Volume 142, 2018), presents an innovative approach to information hiding. The primary focus of the study is on an interpolation-based scheme that employs the modulus function and a re-encoding strategy for concealing information within signals [10]. D.K. Sarmah at el. paper, titled “Improved Cohort Intelligence—A High Capacity, Swift, and Secure Approach on JPEG Image Steganography,” published in the JISA (Volume 45, 2019), presents an advanced method for concealing information within JPEG images. The authors introduce the concept of Improved Cohort Intelligence, emphasizing its attributes of high capacity, speed, and security in the realm of image steganography [11]. X. Duan at el. the paper commences by acknowledging the growing importance of reversible image steganography and the need for effective and secure methods. Duan et al. present their contribution, leveraging a U-Net structure to develop a reversible steganography scheme. The choice of the U-Net architecture is noteworthy, as it has proven effective in various image-processing tasks [13]. P. G. Kuppusamy at el. Paper published in Scalable Computing: Practice and Experience (Volume 21, Number 1, March 2020), presents an innovative technique for image steganography. The authors introduce a novel approach utilizing a modified cycle to enhance the concealment of information within images [14]. Kumar Gaurav’s paper, the unique contribution of the paper lies in the amalgamation of Canny edge detection, dilation operator, and hybrid coding, offering a comprehensive steganographic solution. The author provides a detailed explanation of each component’s role in the concealment process, contributing valuable insights into the proposed methodology [15].

3. Methods and Materials

DiscreteWaveletTransform is applied to the considered image to perform the task and to calculate the parameters. ‘Barb,’ ‘Bluesea,’ ‘Boat,’ ‘Car,’ ‘Leana,’ ‘Loin,’ ‘Mandrill,’ are the names of the cover images that have been used to hide sensitive information as shown in Figure 1 to evaluate the steganographic approach works in this research. practice. These images are of varying sizes and are intended for comparison with the images described in the relevant research.

Cover image C = {p_{ij} for $0 \le I \le X, 0 \le j \le Y$ M be message as D= {m_i for $0 \le i \le k$, where k size and m_i is binary information, two level of DiscreteWaveletTransform of the C calculated using,

[LoLo3, LoHi3, HiLo3, HiHi3] =DiscreteWaveletTransform(C),

[LoLo4, LoHi4, HiLo4, HiHi4] =DiscreteWaveletTransform (HiHi1),

mean=avg (HiHi4),

SF=MF×mean, Multiplier factor (MF) [6].

barb bluesea boat car leena loin mandrrill

Figure 1

Cover Images

4. Proposed Methodology

To increase a low average value, multiply it by a Multiplying Factor to raise its value. Increasing the scaling factor enhances immunity to certain attacks but reduces sensitivity. The PSNR decreases significantly, as will be shown in future investigations [16-17].

Data hiding in the proposed technique is hiding binary data in the DWT matrix in HH2. There are only two possibilities zero and one m_i ε (0,1) at any time. Now this data must be in the HH2 matrix. So next select two neighboring elements P_{ij} and Q_{ij} possibly of in the same row or the same column. Three conditions exist in element value P_{ij}=Q_{ij}, P_{ij}>Q_{ij}, Q_{ij}>P_{ij}. In all cases if m=0 or m=1. If m=0 there must be P_{ij}=Q_{ij}, or P_{ij}>Q_{ij}, or Q_{ij}>P_{ij} If P_{ij}=Q_{ij}, then Q=Q+SF and if Pij>Q_{ij}, P ⇔ Q (Interchange P and Q) and P=P+SF and if Q=Q+SF. Now if m=1, then P_{ij}=Q_{ij}, or P_{ij}>Q_{ij}, or Q_{ij}>P_{ij} if P=Q then P=P+(ScalingFactor), and If P>Q, Then P=P+Q and if Q>P Then P ⇔ Q (Interchange P and Q) and Q=Q+SF [18].

4.1 *Embedding Algorithm*

Step 1: Select original Cover Image C from the database.

Step 2: Obtain 2D DWT of C to get LL1, LH1, HL1 and HH1 using DWT(C)

Step 3: Obtain 2D DWT of HH1 from step2 to get LL2, LH2, HL2 and HH2 using DWT(HH1)

Step 4: Calculate Scaling Factor (SF) from absolute value of mean of HH2.

Step 5: Select the information bit to be embedded m=0 or 1.

Step 6: Select two neighboring coefficients having either of conditions $P_{ij}=Q_{ij}, P_{ij}>Q_{ij}, P_{ij}<Q_{ij}P_{ij}<Q_{ij}$

Step 7: If m=0, and P=Q then Q=Q+SF, and P>Q, P ⇔ Q (Interchange P and Q) and P=P+(ScalingFactor), and Q>P Q=Q+(ScalingFactor)

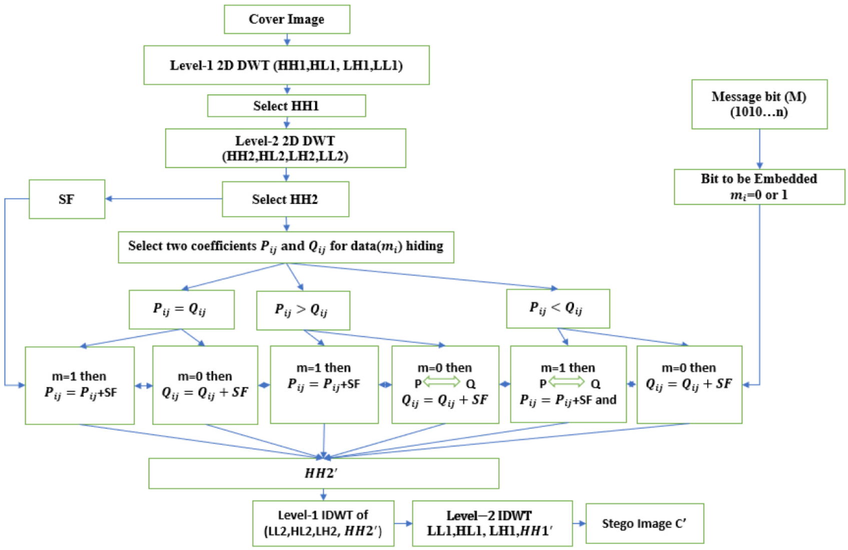

Figure 2

Data Embedding Process

If m=1, make $P_{ij} > Q_{ij}$, And if m=1, and P=Q then P=P+(ScalingFactor), and If P>Q, Then P=P+Q and If Q>P Then P ⇔ Q (Interchange P and Q) and Q=Q+(ScalingFactor)

Step 8: Take Inverse DWT of using HH2′=IDWT (LoLo3, LoHi3, HiLo3 and HiHi3′)

Step 9: Take Inverse DWT of LL1′ using C′=IDWT (LoLo2, LoHi2, HiLo2 and HiHi2′)

4.2 *Extracting Algorithm*

Step 1: Obtain 2D DWT of stego Image (C′) to get LoLo3, LoHi3, HiLo3 and HiHi3′ using DiscreteWaveletTransform(C′)

Step 2: Obtain 2D DiscreteWaveletTransform of HH1′ to get LoLo4, LoHi4, HiLo4 and HiHi4′ using DiscreteWaveletTransform (HH1′)

Step 3: If $P_{ij} > Q_{ij}$, m=1 and if $P_{ij} < Q_{ij}$, m=0

All above steps are shown in Figure 2 and Figure 3 for data hiding and extractions.

5. Comparative Analysis

Transforming the DWT (HiHi2) of a cover image based on binary data could end up resulting in a pixel's representation evolving periodically. The SF is directly related to MultiplyingFactor and Peak Signal Noise Ratio is inversely related to ScalingFactor, as seen in Figure 5. A greater value of SF results in more fluctuation in the HH2 coefficient, leading to a proportionately bigger variation in the pixels of the cover picture after data concealment. The graph indicates a decrease in PSNR at higher MF levels [19-20]. In Table 1, we have tested our approach on seven different cover images. We found that the PSNR and capacity have a similar direction [21-23]. We have compared the proposed technique with existing techniques as shown in Figure 4 and our technique having high PSNR value.

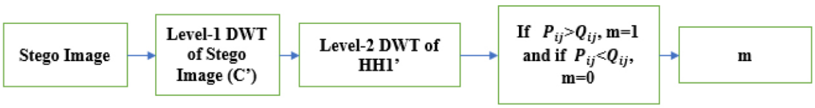

Figure 3

Data Extraction Process

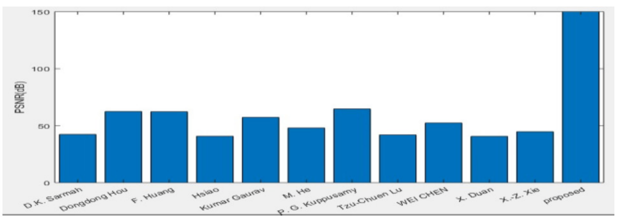

Figure 4

Evaluation of techniques [8-11][13-15][21-23]

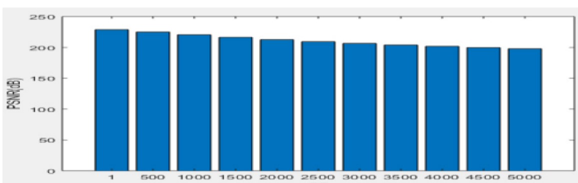

Figure 5

Variation of PSNR with SF

This study encompasses a comprehensive exploration of steganographic attacks, incorporating a diverse range of techniques. The employed attacks, characterized by their additive nature, include Gaussian noise (GN), Salt and Pepper (SP) noise, and compression (10%). The primary objective is achieving the complete recovery of data from the stego images without any errors. Gaussian noise (GN) is introduced with variations in mean values (0, 0.009, 0.09) and variances (0.09, 0.089). Salt and Pepper (SP) noise is applied with varying densities (0.009, 0.016, 0.19, 0.1578). Additionally, JPEG compression is implemented at different percentages (5%, 11%, 14%, 25%). Remarkably, in all instances, the recovery process results in full data retrieval, as illustrated in Figure 6, attesting to the robustness of the approach [7].

Table 1

Parameters with Multiplying Factor

Image	Parameter	MF=1	MF=2	MF=10	MF=25	MF=50	MF=70	MF=100	MF=150
barb	PSNR	196.0635	196.0541	195.9780	195.8302	195.5705	195.3514	195.0056	194.3896
	SSIM	0.9886	0.9886	0.9884	0.9880	0.9872	0.9864	0.9851	0.9823
	Q	0.9856	0.9856	0.9852	0.9842	0.9818	0.9794	0.9750	0.9659
bluesea	PSNR	238.5164	238.5085	238.4447	238.3213	238.1055	237.9241	237.6385	237.1306
	SSIM	0.9992	0.9992	0.9992	0.9991	0.9991	0.9991	0.9990	0.9989
	Q	0.9976	0.9976	0.9975	0.9975	0.9973	0.9972	0.9971	0.9967
boat	PSNR	212.2965	212.2059	211.3864	209.5128	205.9681	203.1346	199.2033	193.6504
	SSIM	0.9969	0.9968	0.9961	0.9938	0.9871	0.9794	0.9642	0.9311
	Q	0.9306	0.9302	0.9193	0.8858	0.8378	0.8098	0.7770	0.7333
car	PSNR	199.1525	199.1089	198.7410	197.9686	196.5045	195.2364	193.2710	190.0370
	SSIM	0.9946	0.9945	0.9940	0.9922	0.9873	0.9817	0.9706	0.9461
	Q	0.9944	0.9943	0.9921	0.9834	0.9602	0.9385	0.9059	0.8572
leena	PSNR	206.9171	206.7133	204.7067	200.1357	192.9604	188.2484	182.5742	175.5226
	SSIM	0.9952	0.9950	0.9917	0.9778	0.9366	0.8927	0.8198	0.7029
	Q	0.9942	0.9936	0.9819	0.9422	0.8704	0.8186	0.7512	0.6606
loin	PSNR	206.4706	206.4516	206.2977	206.0006	205.4829	205.0516	204.3822	203.2252
	SSIM	0.9928	0.9928	0.9927	0.9924	0.9918	0.9913	0.9903	0.9884
	Q	0.9701	0.9701	0.9695	0.9675	0.9617	0.9559	0.9461	0.9297
mandrrill	PSNR	191.5584	191.4505	190.5374	188.6610	185.3830	182.8348	179.3037	174.2531
	SSIM	0.9846	0.9843	0.9817	0.9738	0.9528	0.9305	0.8912	0.8198
	Q	0.9837	0.9831	0.9785	0.9639	0.9347	0.9101	0.8719	0.8118

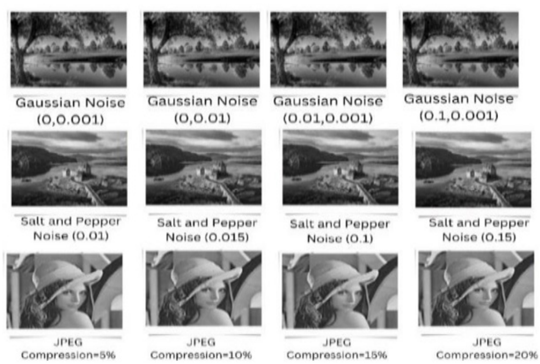

Figure 6

Immunity of Stego-Image against Various Attacks

6. Discussion and Conclusion

Challenges in existing techniques, such as low hiding capacity, visual artifacts, and vulnerability to attacks, are acknowledged. The study aims to address these limitations and emphasizes the significance of achieving high PSNR values. The research claims to introduce an approach that serves as a solution to improve concealing capacity, processing speed, and security, and minimize visual artifacts. In summary, the study seeks to contribute a novel and effective data-concealing technique in the realm of steganography, particularly in digital images, using the DWT approach.

References

[1] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G., Information hiding-a survey. Proceedings of the IEEE, 87(7), 1062-1078 (1999).

[2] Chang, C.C.; Lin, C.C.; Tseng, C.S. Reversible hiding in DCT-based compressed images. *Inf. Sci.* 177, 2768–2786 (2007).

[3] Chi, Cheng, "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition, 37, 469-474 (2004). doi: 10.1016/j.patcog.2003.08.007.

[4] WEI CHEN, Multi-Layer Mini-Sudoku Based High-Capacity Data Hiding Method, *IEEE Access* VOLUME 8 (2020). Digital Object Identifier 10.1109/ACCESS.2020.2986340.

[5] B Singh, "A hybrid algorithm for robust image steganography", Multidimensional Systems and Signal Processing (2020), https://doi.org/10.1007/s11045-020-00725-0.

[6] Pranab, "A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization" *Applied Soft Computing Journal*, https://doi.org/10.1016/j.asoc.2020.106257.

[7] Pratap Chandra, "High-capacity steganography based on IWT using eight-way CVD and *n*-LSB ensuring secure communication", Optik - 167804, https://doi.org/10.1016/j.ijleo.2021.167804.

[8] M. He, "A mini-Sudoku matrix-based data embedding scheme with high payload", *IEEE Access*, vol. 7, pp. 141414-141425 (2019).

[9] X.-Z. Xie, "Extended squared magic matrix for embedding secret information with large payload", *Multimedia Tools Appl.*, vol. 78, no. 14, pp. 19045-19059, Jul. (2019).

[10] Tzu-Chuen Lu, "Interpolation-based hiding scheme using the modulus function and re-encoding strategy", *Signal Processing* 142, 244–259 (2018).

[11] D.K. Sarmah and A.J. Kulkarni, "Improved Cohort Intelligence—A high capacity, swift and secure approach on JPEG image steganography", *Journal of Information Security and Applications* 45, 90–106 (2019).

[12] Patel, C. B., Wandra, K. H., & Shah, S., "Pixel swapping and parity-based image steganography algorithm" In 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-6). IEEE (2016, March).

[13] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a U-Net structure", *IEEE Access*, vol.7, pp. 9314-9323 (2019).

[14] P. G. Kuppusamy, K. C. Ramya, S. Sheebha Rani, "A novel approach based on modified cycle generative adversarial networks for image steganography", *Scalable Comput., Pract. Exper.*, vol. 21, no. 1, pp. 63-72, Mar. (2020).

[15] Kumar Gaurav, "Image steganography based on Canny edge detection, dilation operator and hybrid coding" *Journal of Information Security and Applications* 41, 41–51 (2018), https://doi.org/10.1016/j.jisa.2018.05.001.

[16] Fatemeh Jabbari, "Adaptive multilevel technique based on histogram shifting for eversible data hiding" Multidimensional Systems and Signal Processing, https://doi.org/10.1007/s11045-018-0617-x.

[17] Yih-Kai Lin, A data hiding scheme based upon DCT coefficient modification, Computer Standards & Interfaces 36, 855–862 (2014).

[18] Xiyao Liu, Robust coverless steganography using limited mapping images, *Journal of King Saud University – Computer and Information Sciences* 34, 4472–4482 (2022).

[19] Munthir Bahir Tuieb "Image steganography using Fresnelet transformations, stated coefficients and a pre-processed message" *JDMSC,* Vol. 26, No. 6, pp. 1683–1689 (2023). DOI:10.47974/JDMSC-1614.

[20] Priyank Khare, "A reliable and secure image watermarking algorithm using homomorphic transform in DWT domain", MSSP, https://doi.org/10.1007/s11045-020-00732-1.

[21] F. Huang, X. Qu, H. J. Kim and J. Huang, "Reversible Data Hiding in JPEG Images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 9, pp. 1610-1621, Sept. (2016).

[22] Dongdong Hou, "Reversible Data Hiding in JPEG Image Based on DCT Frequency and Block Selection", Signal Processing (2018).

[23] Hsiao, T.-C.; Liu, D.-X.; Chen, T.-L.; Chen, C.-C. Research on Image Steganography Based on Sudoku Matrix. *Symmetry*, 13, 387 (2021).