Huffman Encoding with White Tailed Eagle Algorithm-based Image Steganography Technique

Sultan Alkhliwi
Department of Computer Science, Faculty of Science, Northern Border University, Saudi Arabia
salkhliwi@nbu.edu.sa
(corresponding author)

Received: 18 November 2022 | Revised: 3 December 2022 | Accepted: 15 February 2023

ABSTRACT

Since the Internet is a medium for transporting sensitive data, the privacy of the message transported has become a major concern. Image steganography has become a prominent tool for hiding data to ensure privacy during transfer. An efficient steganography system is essential to accomplish the best embedding capacity and maintain the other parameters at a satisfying level. Image encryption systems provide a secure and flexible system to maintain the privacy of image conversion and storage in the transmission system. Many existing image steganography methods can be attacked by various techniques, or do not support many image formats for embedding. To resolve these shortcomings, this study presents the Huffman Encoding with White Tailed Eagle Algorithm-based Image Steganography (HEWTEA-IS) technique, aiming to achieve secrecy with no compromise in image quality. The HEWTEA-IS method uses Discrete Wavelet Transform (DWT) for the decomposition of images into different subbands, and Huffman encoding to determine the embedding bits on the decomposed blocks and offer an additional layer of security. Moreover, the WTEA resolves the problem of imperceptibility by identifying the optimal probable position in the cover image for embedding secret bits. The proposed algorithm was simulated and examined in terms of different measures, and an extensive experimental analysis ensured that it is superior to other methods in several aspects.

Keywords-image steganography; embedding process; Huffman encoding; image decomposition; security

I. INTRODUCTION

Steganography is the procedure for embedding secret or confidential data in cover media such as video, text, image, and audio files. Cover mediums with a higher level of redundancy are more suitable for steganography [1, 2]. A digital image can be used as a cover medium to transmit confidential data embedded in the Least Significant Bit (LSB) of a pixel. Steganography can be utilized to securely transmit and store data and can have other applications, such as content authentication, copyright protection, and data integrity assurance [3]. Various data-hiding methods have been explored and several valuable steganographic methods have been proposed to improve security and protect data against unauthorized access [4, 5]. In information-hiding mechanisms, the three quality parameters considered are robustness, capacity, and imperceptibility [6]. These parameters are very important in image steganography. Robustness determines the degree of security from hackers or eavesdroppers during data transmission, imperceptibility means that the hidden information and the original cover image are indistinct, and capacity defines the amount of hidden data or image size that is transferred [7-10].

An image steganography method is generally assessed from five different aspects: computational costs, perceptual transparency (visual quality), temper resistance, payload (embedding) capacity, and security. Visual quality is regarded as good whenever the variance between the stego and the original image can be invisible to the Human Vision System (HVS) [11]. The embedding capacity is determined by the volume of data hidden in the cover images and can be measured by Bits Per Pixel (BPP). A high payload permits a high confidential data insertion into the host images. Security is the capacity of a mechanism to protect confidential data from any intruder. Image steganography can provide superior imperceptibility and payload [12]. Steganography methods having less distorted stego images are much more secure compared to others with more distortion, as they do not allure the attention of an intruder [13-15]. An ideal steganographic method must have a large embedding capacity and outstanding visual quality. But, as visual quality can be the inverse proportion of embedding capability, increasing one variable results in massive compromise on the other.

In [16], a higher-capacity image steganography method was introduced utilizing GA. This method used LSB replacement steganography to embed confidential data. But confidential

data can be modified and rearranged by previously encoding them in the LSBs of cover imageries. The variables utilized for rearranging and modifying the confidential data could be managed by the GA. A unique idea named flexible chromosomes was presented, which permitted GA to interpret chromosome values in distinct techniques. GA tried to discover the optimal variable values that have a high visual quality in the stego images. In [17], an image steganography method related to Integer Wavelet Transform (IWT) was presented. Using IWT, the cover image was converted to suppress the confidential message into the HL, HH, and LH frequency bands of the cover image. According to their Most Significant Bits (MSBs), the coefficients of these bands were labeled into 6 classes. All coefficients from various bands belonging to the same class were gathered. The embedding procedure was initiated from the highest class by supervising the coefficients to match the secret message size. In [18], an image steganography method was presented that used LSB and secret map methods by implementing 3D chaotic maps, such as 3D logistic and Chebyshev maps, to improve security. This approach utilized the idea of performing random insertion and choosing a pixel from a host image. In [19], a novel hybrid technique named Compressed Encrypted Data Embedding (CEDE) was presented. In this method, the confidential data were initially compressed with the Lempel-Ziv-Welch (LZW) compressing method. The compressed secret data were encoded using Advanced Encryption Standard (AES) symmetric block ciphers. In the final stage, the encoded data were encoded into 512×512 pixel images. The encoded and compressed secret data bits were split into sets of two bits, and the cover image pixels were also ordered in four pairs. In [20], a steganography method was presented that utilized chaos theory and PSO targeting to identify the optimal pixel in the cover image to hide confidential data while maintaining the prominence of the resulting stego images. To enhance embedding capacity, the secret and host images could be split into blocks that stored a suitable amount of secret bits. In [21], a DL-related steganography method was presented, using a deep supervised edge detector and CNN to retain more edge pixels than traditional edge-detection methods. The cover images were preprocessed by masking the latter 5 bits of all pixels, and the edge detector was used to obtain a grayscale edge map. In [22], emphasis was placed on improving the secret-sharing approach to enhance security along with simplicity and fast computation. This study solved certain published flaws in the share reconstruction stage by suggesting a new distribution method to increase security and authenticity.

The current study proposes Huffman Encoding with White Tailed Eagle Algorithm for Image Steganography (HEWTEA-IS). This method uses the Discrete Wavelet Transform (DWT) to decompose images into different subbands, Huffman encoding to determine the embedding bits on the decomposed blocks and offer an additional layer of security, and White Tailed Eagle Algorithm (WTEA) to resolve the problem of imperceptibility by identifying the optimal probable position in the cover image to embed secret bits. The proposed method was simulated and examined with various measures.

II. PROPOSED MODEL

The proposed HEWTEA-IS method aims to achieve secrecy without compromising image quality. The HEWTEA-IS method encompasses different subprocesses, namely DWT-based image decomposition, embedding, Huffman encoding, WTEA-based pixel selection, and extraction.

A. Image Decomposition

The cover image is decomposed into different subbands. Wavelet Transforms (WT) can be used to identify individual locations in host images to hide confidential data [23]. These regions of the host image that are minimum sensible to HVS are recognized as frequency bands. The hidden data in these bands do not degrade the quality of the visual image significantly. These bands continuously comprise data on texture, edge, and sharp transitions of images. The Haar DWT coefficient was calculated horizontally and vertically. In horizontal, an image was decomposed to High-(H) and Low-(L) frequency bands, where L was computed by taking the average of 2 sequential pixels horizontally, and H by taking the variance between them. In vertical, L and H were again decomposed into 4 distinct subbands using High-Low (HL), Low-Low (LL), High-High (HH), and Low-High (LH) by taking the average and the variance between two vertically sequential pixels. The superior magnitudes of the wavelet coefficient show the most important data of the images. The magnitudes of the LL coefficients were superior to the other subbands (HH, LH, and HL) and comprise the smooth and plane region of an image that is extremely sensitive to human eyes. Thus, embedding even little data into the LL subbands results in maximum distortion. The other three subbands comprise edge details and sharp transitions in images. So, the data should be embedded in these three subbands. The Haar DWT coefficient was computed using pairwise average and variance as shown in (1) and (2):

$$S_{1,n} = \frac{(S_{0,2n}+S_{0,2n+1})}{2}; \quad D_{1,n} = S_{0,2n+1} - S_{0,2n} \qquad (1)$$

The inverse of Haar DWT was computed by:

$$S_{0,2n} = S_{1,n} + \frac{D_{1,n}}{2}; \quad S_{0,2n+1} = S_{1,n} - \frac{D_{1,n}}{2} \qquad (2)$$

At this point, $S_{0,2n}$, $S_{0,2n+1}$ are the sequential pixel values of cover images.

B. Embedding Process

Normally, the WTEA begins the search with an arbitrarily selected initial population. Using a fitness function, these randomly generated solutions are evaluated throughout iterations and are enhanced via a set of formulas until an ending condition is met. However, despite the differences between population-based methods, this technique shares baseline data. In this study, the search procedure was divided into exploration and exploitation stages [24]. Exploration includes searching the region for an open location that is farther from the existing location. The exploration phase takes place when a metaheuristic algorithm tries to find a better area. At the same time, exploitation explores the near-optimum point, focusing on the neighborhood of high-quality answers inside the search space. Executing exploration alone might lead to a

novel location with a poor degree of precision, while exploitation increases the risk of getting trapped in local optima. Several studies emphasized the importance of balancing exploitation and exploration in metaheuristic algorithms. Consequently, it is crucial to achieving an accurate balance between these two phases. This study used two different stages to carry out efficient exploitation and exploration. The WTEA step-by-step method can be described as:

- Step 1 - Population initialization: WTEA, begins the investigation via a set of randomly produced components (a set of eagles with a random location):

$$E_i = lb_i + rand \times (ub_i - lb_j); \quad i = 1,2,\dots,N \quad (3)$$

where E_i is the location of the i-th eagle, ub_i and lb_i are the lower and upper boundaries, respectively, and *rand* represents a random number within [0,1].

- Step 2 - Population assessment: In this stage, the randomly generated solution is evaluated through a fitness function, and the eagle with optimal fitness value is selected as E_{Best}.
- Step 3 - Searching phase (exploration): White-tailed eagles search for prey within the search region they have chosen and move in diverse directions to accelerate their hunt. This process explores different regions using its randomized operator. Every eagle collaborates with the best and randomly interacts with others to upgrade the location. Figure 1 shows the steps involved in WTEA. This behavior is determined by:

$$E_i(t+1) = \begin{cases} E_i(t) + 2 \times r_1 \times (E_r(t) - E(t)) & if\ r_2 < 0.5 \\ E_i(t) + 2 \times r_1 \times (E_{Best}(t) - E_j(t)) & if\ r_2 \geq 0.5 \end{cases} \quad (4)$$

where $E_i(t)$ is the location of i-th eagle in the search space at iteration t, E_{Best} is the location of the better eagle (adjacent to the prey), and r_1 and r_2 are random numbers within [0,1].

- Step 4 - Improving phase (exploitation): Every eagle gets knowledge from the best candidate in the population. To improve the quality of the WTEA solution, every eagle interacts with the better eagle of the swarm E_{Best}, which has the highest influence on others to discover the prey:

$$E_i(t+1) = rand \times E_{Best}(t) + rand \times (E_{Best}(t) - E_i(t)) \quad (5)$$

- Step 5 - Movement limitation: In all iterations, WTEA alters the distance every eagle moves through every dimension of the scratch region. Equations (4) and (5) show that eagle movement is a stochastic parameter and could allow the eagle to follow a large distance. Consequently, to accomplish this oscillation and prevent the eagle divergence, any eagle that goes beyond the search space limit would be reproduced based on:

$$E_i = \begin{cases} lb_i & if\ E_i \leq lb_i \\ ub_i & if\ E_i \geq ub_i \\ E_j & \text{otherwise} \end{cases} \quad (6)$$

This model is used to select the best pixels to hide private information [25]. The optimum location is found by using the WTEA approach that implements initialization by arbitrarily choosing particles and later searching for the better fit by upgrading each particle position. Initially, the population is chosen at random, and the location is upgraded through the objective function. Next, the better solution gets recognized to embed information. The original cover image is considered as O with $M \times N$ dimensions. Usually, the image can be described by a spatial representation. DWT is applied to convert them into a frequency domain. Then, the image undergoes sampling and decomposition to provide a higher degree of robustness as:

$$[O_1 O_2 O_3 O_4] = DWT(O) \quad (7)$$

where O_1 represents the coefficient of the lower frequency band and comprises each substantial data of the image, O_2, O_3, and O_4 indicate the higher-frequency bands and represent data such as edges of the image. The O_1 band is carefully chosen for additional processing and the coefficient is extracted as:

$$[O_1^{LL}\ O_1^{LH}\ O_1^{HL}\ O_1^{HH}] = DWT(O_1) \quad (8)$$

where O_1^{LL} indicates the low-frequency subband, and O_1^{LH}, O_1^{HL}, and O_1^{HH} denote the high-frequency subbands of O_1. Then, the stego image is created by:

$$C_1^{*j} = C_1^j + (D_i \times P_{opt}) \quad (9)$$

where D_j indicates the secret textual information, and P_{opt} is the optimal location for embedding the information. Inverse DWT is executed to characterize the image after data hiding:

$$O_1^{**} = IDWT(O_1^{*LL} O_1^{*LH} O_1^{*HL} O_1^{*HH}) \quad (10)$$

The embedded secret information with the adapted band is:

$$O^{**} = IDWT(O_1^{**} O_2 O_3 O_4) \quad (11)$$

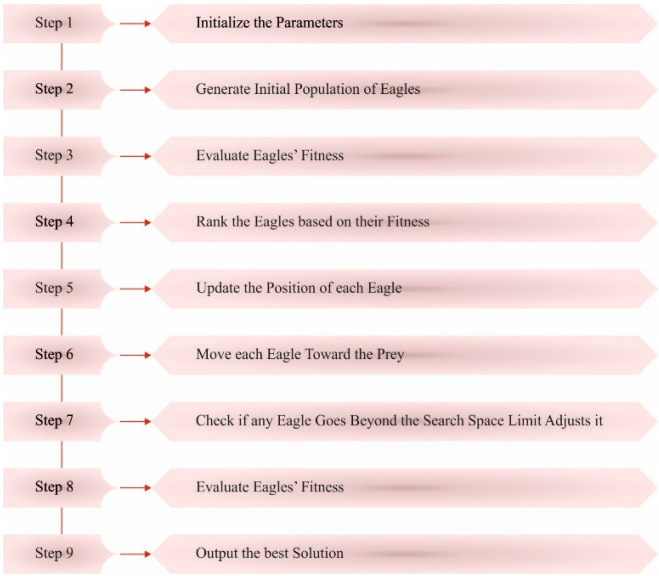

Fig. 1. Steps involved in WTEA

C. Huffman Encoding

Huffman coding is a lossless data compression technique. Its objective is to allocate parameter-length code to input characters, as the length of the assigned code depends on the

frequency of the characters [26]. The more common character gets a smaller code, and the less common character gets a larger one. The parameter length code assigned to each input character is a prefix code, which implies that a code is assigned so that it is not the prefix assigned to any other. Huffman coding ensures that there is no ambiguity while decoding the bit stream.

1. Generate a leaf node for all input characters and construct a minimum heap of each leaf node.
2. For the minimum heap, obtain the topmost two nodes (N1 and N2) with the least frequency.
3. Generate a novel internal node N3 with a frequency equivalent to the sum of frequencies of nodes N1 and N2. Make N1 the left and N2 the right child of N3. A new node N3 is added to the minimum heap.
4. Repeat steps 2 and 3 until the minimum heap has a single node.

D. Extraction Process

The objective is to successfully extract the secret messages from the input stego images on the receiver. The stego image undergoes DWT to transform it from spatial to frequency representation. The stego images are indicated as O^{**R}:

$$[O_1^{**R} O_2^{**R} O_3^{**R} O_4^{**R}] = DWT(O^{**R}) \quad (12)$$

The modified band is O_1^{**R}, therefore the coefficient of the sub-band is:

$$\left[o_1^{LL_R^*} O_1^{LH_R^*} 0_1^{HL_R^*} O_1^{HH_R^*}\right] = DWT(O_1^{**R}) \quad (13)$$

Next, match the secret key and once it matches, the original secret message is extracted. WTEA is applied to locate the position of hidden information, and Huffman decoding is applied to extract the secret message. Thus, the stego image is attained in binary format. When the secret keys don't match, an encrypted image is received. The encrypted images are produced for adding another level of security to the system.

III. RESULTS AND DISCUSSION

This section examines the security performance of the HEWTEA-IS algorithm on several images from the USC-SIPI repository [27]. The experimental values were assessed under varying Message Sizes (MS).Table I shows a result analysis of the HEWTEA-IS method under variable message sizes and images. The HEWTEA-IS model showed a good performance in all images. Figure 3 provides the results of the HEWTEA-IS method with different message sizes using Image 1. In this image, the HEWTEA-IS method gained an average MSE of 0.00012, an average PSNR of 126.36dB, an average BER of 0.033, and an average SSIM of 0.9993.

Figures 4, 5, and 6 show the results of the HEWTEA-IS method with different message sizes in Images 2 and 3. In these images, the HEWTEA-IS system achieved average MSE of 0.00011, 0.00013, and 0.00012, average PSNR of 127.05, 126.18, and 126.94dB, average BER of 0.035, 0.0034, and 0.032, and average SSIM of 0.9995, 0.9994, and 0.9995, respectively.

TABLE I. RESULTS ANALYSIS OF HEWTEA-IS APPROACH WITH DISTINCT IMAGES AND MEASURES

Images	Message size (KB)	MSE	PSNR (dB)	BER	SSIM
Image 1	50	0.00012	126.55	0.028	0.9992
	100	0.00011	127.30	0.035	0.9993
	150	0.00014	125.21	0.031	0.9995
	200	0.00015	124.61	0.042	0.9991
	250	0.00010	128.13	0.031	0.9994
Average		0.00012	126.36	0.033	0.9993
Image 2	50	0.00011	127.30	0.038	0.9994
	100	0.00010	128.13	0.034	0.9992
	150	0.00014	125.21	0.038	0.9998
	200	0.00011	127.30	0.029	0.9995
	250	0.00011	127.30	0.036	0.9996
Average		0.00011	127.05	0.035	0.9995
Image 3	50	0.00011	127.30	0.039	0.9991
	100	0.00015	124.61	0.037	0.9998
	150	0.00013	125.85	0.032	0.9997
	200	0.00011	127.30	0.030	0.9992
	250	0.00013	125.85	0.034	0.9992
Average		0.00013	126.18	0.034	0.9994
Image 4	50	0.00010	128.13	0.032	0.9998
	100	0.00015	124.61	0.029	0.9992
	150	0.00011	127.30	0.034	0.9997
	200	0.00012	126.55	0.031	0.9994
	250	0.00010	128.13	0.036	0.9992
Average		0.00012	126.94	0.032	0.9995

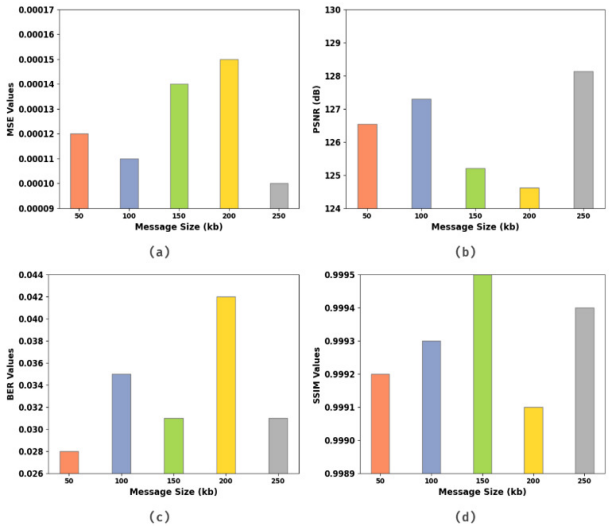

Fig. 2. Classification analysis of the HEWTEA-IS algorithm in Image 1: (a) MSE, (b) PSNR, (c) BER, (d) SSIM.

Table II shows the comparative results of the HEWTEA-IS with other recent methods, and Figure 7 shows a visual PSNR analysis of HEWTEA-IS with them. The HEWTEA-IS achieved the highest PSNR value of 126.634dB, HPSO and Huffman-PSO models had close PSNR values, while the PSO-DWT and PSO algorithms had the least PSNR values.

Figure 8 shows a comparative SSIM investigation of the HEWTEA-IS. The HEWTEA-IS had the highest SSIM of 0.9994, the HPSO and Huffman-PSO algorithms had close SSIM values, while PSO-DWT and PSO had the least SSIM.

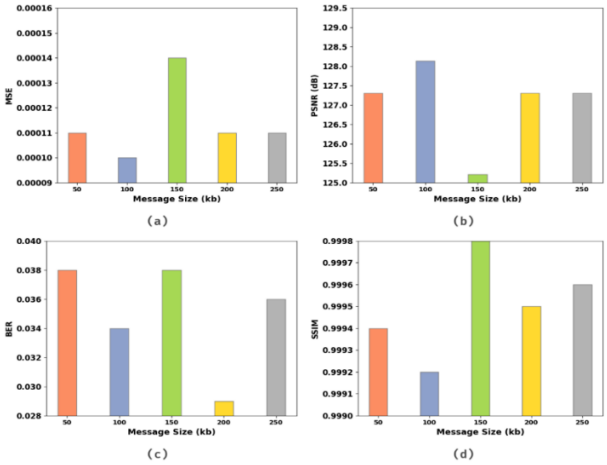

Fig. 3. Classification analysis of the HEWTEA-IS algorithm in Image 2: (a) MSE, (b) PSNR, (c) BER, (d) SSIM.

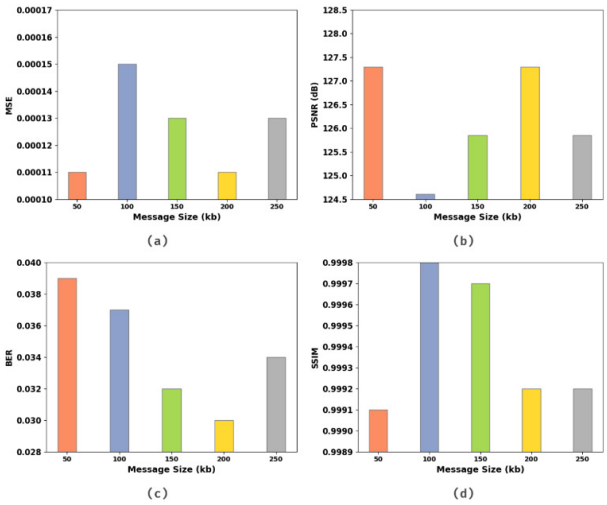

Fig. 4. Classification analysis of the HEWTEA-IS algorithm in Image 3: (a) MSE, (b) PSNR, (c) BER, (d) SSIM.

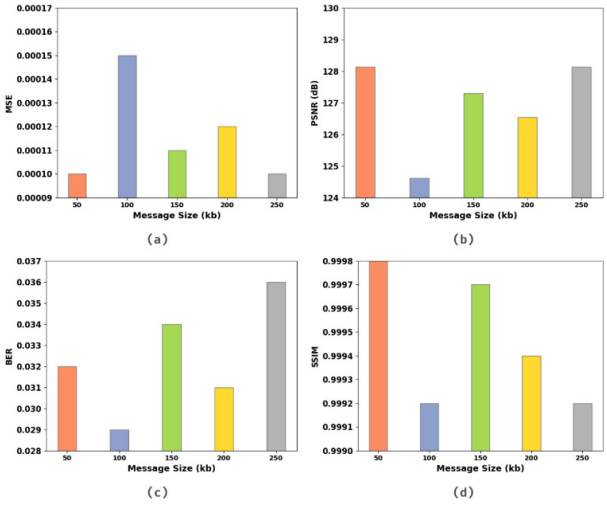

Fig. 5. Classification analysis of the HEWTEA-IS algorithm in Image 4: (a) MSE, (b) PSNR, (c) BER, (d) SSIM.

TABLE II. COMPARISON OF HEWTEA-IS WITH OTHER METHODS

Methods	MSE	PSNR (dB)	BER	SSIM
HEWTEA-IS	0.00012	126.634	0.0338	0.9994
PSO	4.26800	35.526	0.0520	0.9597
HPSO	0.00200	102.110	0.0492	0.9857
PSO-DWT	0.73000	50.864	0.0498	0.9764
Huffman-PSO	0.00020	122.110	0.0413	0.9935

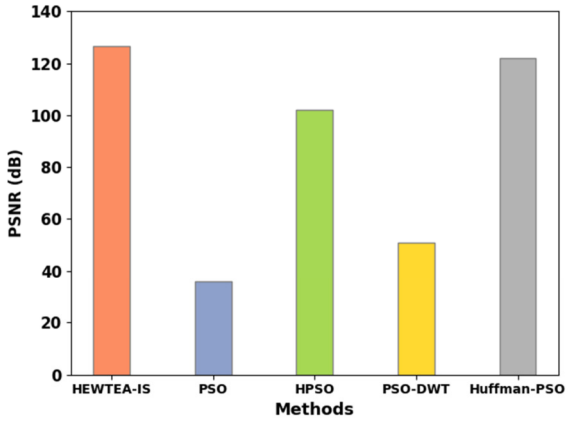

Fig. 6. PSNR analysis of the HEWTEA-IS with recent methods.

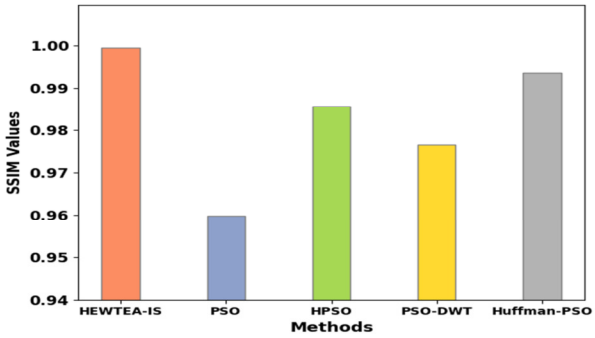

Fig. 7. SSIM analysis of the HEWTEA-IS with other methods.

Figure 9 shows a detailed BER comparison of the HEWTEA-IS. The HEWTEA-IS had the least BER of 0.0338, while PSO, HPSO, PSO-DWT, and Huffman-PSO had increased BER of 0.0520, 0.0492, 0.0498, and 0.0413, respectively. These results affirmed the superiority of the HEWTEA-IS method.

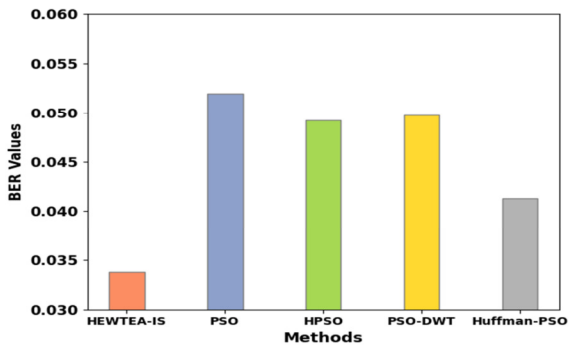

Fig. 8. BER analysis of the HEWTEA-IS with other methods.

IV. CONCLUSION

This study presented the novel Huffman Encoding with White Tailed Eagle Algorithm for Image Steganography (HEWTEA-IS) with the purpose of achieving secrecy without compromising image quality. The proposed method used Discrete Wavelet Transform (DWT) for the decomposition of images into different subbands, Huffman encoding to determine the embedding bits on the decomposed blocks and offer an additional layer of security, and WTEA to resolve the problem of imperceptibility by identifying the optimal positions in the cover images for embedding secret bits. The proposed method was experimentally analyzed and compared to other recent methods in several aspects, showing its superiority. In the future, the HEWTEA-IS can be extended to audio messages.

REFERENCES

[1] B. Lakshmi Sirisha and B. Chandra Mohan, "Review on spatial domain image steganography techniques," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1873–1883, Aug. 2021, https://doi.org/10.1080/09720529.2021.1962025.

[2] H. G. Zaini, "Image Segmentation to Secure LSB2 Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 11, no. 1, pp. 6632–6636, Feb. 2021, https://doi.org/10.48084/etasr.3859.

[3] V. K. Sharma, P. C. Sharma, H. Goud, and A. Singh, "Hilbert quantum image scrambling and graph signal processing-based image steganography," *Multimedia Tools and Applications*, vol. 81, no. 13, pp. 17817–17830, May 2022, https://doi.org/10.1007/s11042-022-12426-w.

[4] M. Tarhda, R. E. Gouri, and L. Hlou, "Implementation of an Optimized Steganography Technique over TCP/IP and Tests Against Well-Known Security Equipment," *Engineering, Technology & Applied Science Research*, vol. 8, no. 6, pp. 3515–3520, Dec. 2018, https://doi.org/10.48084/etasr.2334.

[5] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 357–366, Feb. 2020, https://doi.org/10.1080/09720502.2020.1731949.

[6] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, Part B, pp. 3559–3568, Jun. 2022, https://doi.org/10.1016/j.jksuci.2020.12.017.

[7] W. Alexan, M. E. Beheiry, and O. Gamal-Eldin, "A Comparative Study Among Different Mathematical Sequences in 3D Image Steganography.," *International Journal of Computing and Digital Systems*, vol. 9, no. 4, pp. 545–553, Jul. 2020.

[8] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, https://doi.org/10.48084/etasr.2380.

[9] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021, https://doi.org/10.1109/ACCESS.2021.3053998.

[10] J. Khandelwal, V. K. Sharma, J. K. Raguru, and H. Goyal, "Recent Trend of Transform Domain Image Steganography Technique for Secret Sharing," in *Cyber Warfare, Security and Space Research*, Jaipur, India, 2022, pp. 171–185, https://doi.org/10.1007/978-3-031-15784-4_14.

[11] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Information Security Journal: A Global Perspective*, vol. 30, no. 2, pp. 63–87, Mar. 2021, https://doi.org/10.1080/19393555.2020.1801911.

[12] S. Pramanik and S. Suresh Raja, "A Secured Image Steganography Using Genetic Algorithm," *Advances in Mathematics: Scientific Journal*, vol. 9, no. 7, pp. 4533–4541, Jul. 2020, https://doi.org/10.37418/amsj.9.7.22.

[13] A. Gaffar, A. B. Joshi, S. Singh, and K. Srivastava, "A high capacity multi-image steganography technique based on golden ratio and non-subsampled contourlet transform," *Multimedia Tools and Applications*, vol. 81, no. 17, pp. 24449–24476, Jul. 2022, https://doi.org/10.1007/s11042-022-12246-y.

[14] R. Mansour and M. Girgis, "Steganography-Based Transmission of Medical Images Over Unsecure Network for Telemedicine Applications," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 4069–4085, 2021, https://doi.org/10.32604/cmc.2021.017064.

[15] S. Alsubai, M. Hamdi, S. Abdel-Khalek, A. Alqahtani, A. Binbusayyis, and R. F. Mansour, "Bald eagle search optimization with deep transfer learning enabled age-invariant face recognition model," *Image and Vision Computing*, vol. 126, Oct. 2022, Art. no. 104545, https://doi.org/10.1016/j.imavis.2022.104545.

[16] P. D. Shah and R. S. Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Engineering Science and Technology, an International Journal*, vol. 24, no. 3, pp. 782–794, Jun. 2021, https://doi.org/10.1016/j.jestch.2020.11.008.

[17] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13133–13144, Jun. 2018, https://doi.org/10.1007/s11042-017-4935-z.

[18] Maisa'a Abid Ali K. Al-Dabbas; Ashwaq Alabaichi; Adnan Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935–946, Feb. 2020.

[19] A. Hamza, D. Shehzad, M. S. Sarfraz, U. Habib, and N. Shafi, "Novel Secure Hybrid Image Steganography Technique Based on Pattern Matching," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, no. 3, pp. 1051–1077, 2021, https://doi.org/10.3837/tiis.2021.03.013.

[20] A. Jaradat, E. Taqieddin, and M. Mowafi, "A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization," *Security and Communication Networks*, vol. 2021, Jun. 2021, Art. no. e6679284, https://doi.org/10.1155/2021/6679284.

[21] B. Ray, S. Mukhopadhyay, S. Hossain, S. K. Ghosal, and R. Sarkar, "Image steganography using deep learning based edge detection," *Multimedia Tools and Applications*, vol. 80, no. 24, pp. 33475–33503, Oct. 2021, https://doi.org/10.1007/s11042-021-11177-4.

[22] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7951–7985, Mar. 2020, https://doi.org/10.1007/s11042-019-08427-x.

[23] P. K. Muhuri, Z. Ashraf, and S. Goel, "A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization," *Applied Soft Computing*, vol. 92, Jul. 2020, Art. no. 106257, https://doi.org/10.1016/j.asoc.2020.106257.

[24] B. Arandian, A. Iraji, H. Alaei, S. Keawsawasvong, and M. L. Nehdi, "White-Tailed Eagle Algorithm for Global Optimization and Low-Cost and Low-CO2 Emission Design of Retaining Structures," *Sustainability*, vol. 14, no. 17, Jan. 2022, Art. no. 10673, https://doi.org/10.3390/su141710673.

[25] N. Sharma and U. Batra, "An enhanced Huffman-PSO based image optimization algorithm for image steganography," *Genetic Programming and Evolvable Machines*, vol. 22, no. 2, pp. 189–205, Jun. 2021, https://doi.org/10.1007/s10710-020-09396-z.

[26] G. P. Pandey, "Implementation of DNA Cryptography in Cloud Computing and Using Huffman Algorithm, Socket Programming and New Approach to Secure Cloud Data." Rochester, NY, Aug. 07, 2019, https://doi.org/10.2139/ssrn.3501494.

[27] "SIPI Image Database." https://sipi.usc.edu/database/database.php.

AUTHORS PROFILE

Sultan Alkhliwi received his B.E. degree from the Northern Border University in 2008. He received an M.Sc. and Ph.D. from the University of Manchester- U.K in 2013 and 2018, respectively. Currently, he works as an Assistant Professor in Computer Science Department, Faculty of Science, Northern Border University, Saudi Arabia. His research interests include multi-hop communication networks, cryptography, network security, and information security.