Image Steganography Based on NR-Polar DCSK System over Multipath Fading Channel

Noor Dheyaa Majeed, Ali Jaber Al-Askery, and Fadhil Sahib Hasan

***Abstract*—Protecting sensitive data has become an urgent necessity in wireless communication, which predates the emergence of Internet development, where signals transmitted over a channel are distorted by fading, noise, attackers, and interference, which leads to the loss of sensitive information. This paper introduces an efficient approach for image steganography over a wireless channel based on the New Radio (NR) polar code with Differential Chaos Shift Keying (DCSK) modulation to protect secret information over a Rayleigh fading model in the presence of an Additive White Gaussian Noise (AWGN) channel. The DCSK is a non-coherent detection method widely used in broad-spectrum communications due to its high security and effectiveness against fading. On the other hand, steganography is one of the most essential techniques for protecting secret information by embedding it in multimedia. In this work, the secret images are hidden in cover stego using the Least Significant Bits (LSB) technique. The simulation outcomes indicate that the Bit Error Rate (BER) is improved by 8 dB gain in this design over the AWGN channel and approximately 4 dB over the combination channel of AWGN and Rayleigh fading. Besides that, the Peak Signal to Noise Ratio (PSNR) reached 80.2750 dB at 26 dB SNR with 32 Spread Factor (SF). This work introduces a hybrid data protection system that consists of steganography and DCSK techniques, where the data has effectively been retrieved by the receiver.**

***Index terms*—NR polar code, DCSK modulation, AWGN, Rayleigh fading, Steganography, LSB, Secret image.**

I. INTRODUCTION

With the rise of distributed control systems and virtual cloud servers, the amount of data transmitted over the Internet has skyrocketed in the last decade, making safeguarding this sensitive information of paramount importance [1]. Steganography, a domain of information concealment, is employed to embed private data within cover media such as images, text, audio, and videos [2]. The embedding operation is a crucial step in steganography approaches, where any error can compromise the integrity of the image [3]. There are two primary methods for embedding sensitive information into a cover medium [4].

The popular category of embedding is the spatial domain, which involves executing the embedding operation directly within pixels, such as Pixel Value Differencing (PVD) and Least Significant Bits (LSB). This type is characterized by fast execution and simple implementation [5]. The second category is frequency domains, where the pixels of the cover image are converted into frequency representations such as the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). This kind, despite its intricate structure, has significant resistance to incursions [6].

Despite using steganography, the secret data remains at risk of being lost during wireless communication due to various factors such as fading, interference, attackers, and noise, all of which contribute to a high BER [7]. So, the encoding of channels became an essential component of any communication network, where it incorporates redundancy bits into the source message, enabling the decoder to identify and rectify a specific number of mistakes depending on that redundancy [8]. Polar Code is one of the most important kinds of encoding, which can provide channel capacity and relies on minimal encoding and decoding complexity, where it has garnered significant interest from both academia and business over the past decade, leading to their selection as the channel coding scheme in the 5th generation wireless networks (5G) standardization process by the 3rd Generation Partnership Project (3GPP) [9].

The concluding phase of the data transmission in polarization coding is modulation, where a traditional sinusoidal carrier may be substituted with a chaotic carrier to attain enhanced modulation security [10]. The primary benefit of utilizing chaos theory with modulation techniques is achieving pseudo-random behavior, which offers anti-fading and anti-detection capabilities, as well as tolerance to multipath losses [11]. Chaotic systems seem random; nonetheless, they are deterministic and exhibit sensitivity to initial circumstances, meaning that a minor alteration at the outset of the repetitions produces a configuration markedly different from the anticipated waveforms [12]. This renders them unpredictable in the long term if the design factors, such as initial circumstances, sample size, and numerical approach, are not precisely known [13].

The rest of this paper can be summarized as follows: Section II displays the related works. Section III explains the background of the polar code. Section IV describes the proposed approach. Section V discusses and analyzes the results. Section VI summarizes the conclusion of this work.

II. RELATED RESEARCH

The safeguarding of data against loss during transmission has garnered significant interest from researchers; for example, in [14], Banerjee and Jana introduced a steganography framework utilizing Reed Solomon (RS) codes, which are a

Manuscript received June 5, 2025; revised October 14, 2025. Date of publication January 12, 2026. Date of current version January 12, 2026.

N. D. Majeed, and A. J. Al-Askery are with the Technical Engineering College of Artificial Intelligence, Middle Technical University, Baghdad, Iraq (e-mails: noor.dheyaa@mtu.edu.iq, a.alaskery@mtu.edu.iq). F. S. Hasan is with the Department of Electrical Engineering, Mustansiriyah University, Baghdad, Iraq (e-mail: fadel_sahib@uomustansiriyah.edu.iq).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0074

form of non-binary cyclic maximum distance separable codes. Linear interpolation is employed to add two additional pixels to a block of five pixels, hence preserving the encoding polynomial when divided by the generating polynomial. In [15], Lu et al. introduced a robust JPEG steganography technique by utilizing an autoencoder in combination with adaptive Bose-Chaudhuri-Hocquenghem encoding (BCH). In [16], Wang et al. proposed a steganography technique that employs Hamming coding and least significant bit (LSB) substitution. Considering that the sharp sections of the image might undergo more modifications than the smooth areas, a greater volume of concealed messages is embedded in the edge regions, but a negligible amount of information is present in the smooth regions. In [17], Ying et al. enhanced the Syndrome-Trellis Code (STC) coding procedure to develop a steganography technique. This approach modifies the average embedding alteration probability of interconnected elements by modifying submatrices. In [18], Hao et al. Introduced image steganography transmission based on polar code over a fading channel. Quadrature Phase Shift Keying (QPSK) modulation is used in the work. In [19], Alharbi suggested a steganography approach over the AWGN channel based on a convolutional encoder. The Discrete Cosine Transform (DCT) is used to embed the secret message bits. In [20], Li et al. presented an improved near-optimal steganographic coding approach utilizing polar codes and the Successive Cancellation List (SCL) decoding algorithm to reduce additive distortion in steganography, where, the proposed Steganographic selects the parity-check matrix by utilizing the embedding payload as the initial value of Arikan's heuristic and calculates the decoding channel metric based on the optimal modification probability of the minimal distortion model. In [21], Yao et al. suggested a robust design of steganography based on coding of nested polar system over the Binary System Channel (BSC). In [22], Guan et al. presented a steganography design based on Non-Binary Polar Codes (NBPC). The system executes multi-stages of steganography, which is characterized by avoiding the allocation insert redundant problem.

Previous studies have aimed to protect secret data during wireless transmission. However, most prior works have a complex structure of error correction techniques, so these approaches are not suitable for transmitted applications. On the other hand, the previous works fail to consider the influence of fading on traditional modulation. Moreover, the previous research didn't incorporate the secure image of steganography with a reliable channel coding system based on spread spectrum techniques to protect the secret image from attackers and the fading effect.

This paper introduced a novel steganography approach based on polar code to improve reliable data transmission over wireless channels. It incorporates the secure image of steganography with a reliable channel coding system based on spread spectrum techniques to protect the secret image from attackers and the fading effect, where the traditional modulation was replaced with DCSK modulation. Moreover, this modulation isn't needed for synchronization between the sender and receiver sides.

III. Polar Coding Procedure

Polar codes are a kind of capacity-achieving code introduced by Arıkan in 2009 [23]. This code has gained popularity in academia and industry during the past decade, where it is being used as channel coding for uplink and downlink control information in the 3GPP's 5th generation wireless systems (5G) standardization process for enhanced mobile broadband (eMBB) communication services [24]. Polar code works based on the polarization principle, which operates by transforming channels into either reliable (approximately error-free) or entirely unreliable (frozen bits) channels [25]. The Bhattacharyya measure and mutual information chain rule facilitate the evaluation of a polarized channel's reliability and examine the temporal enhancement of polar codes [26]. Furthermore, this FEC coding of the polar code is a concatenated design because it applies the Cyclic Redundancy Check (CRC) to improve the efficiency of error correction. Equation (1) describes the mathematical model of the NR-polar codeword.

$$C = x_l^M G_n^{\otimes} m \tag{1}$$

Let's $x_l^M = (x1, x2, \ldots, xM)$ represent the data sequence and m Kronecker power of G_n, where G_n acts as the kernel matrix, which is described in equation (2) based on G_8. Moreover, the encoder's hardware design is shown in Fig. 1, where C is a data channel [27].

$$G_8 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{2}$$

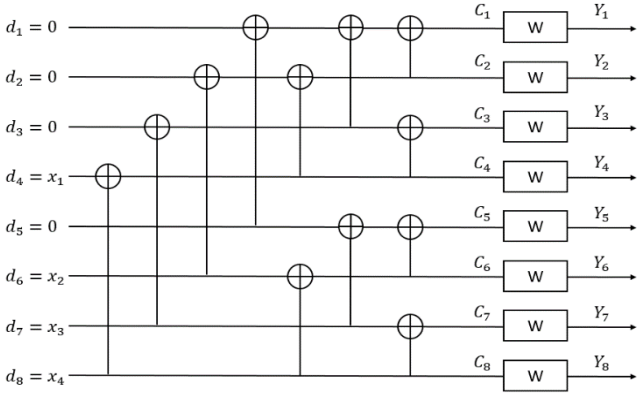

Fig. 1. The construction of a polar encoder for codeword length 8.

In the receiver, there are two types of decoders in polar codes: Successive Cancellation (SC) and Successive Cancellation List (SCL).

The SC decoder employs a "successive cancellation" method to iteratively estimate the bit values. Utilizing the incoming signal and the decoder's previous estimations of the other bits, it assesses the likelihood that each bit is either a 1 or a 0 [28]. This decoder generates an estimated value of $\hat{x}_1^i$ at the receiver using the log-likelihood ratio (LLR), which can be derived from the following equations:

$$L_M^{(i)}(y_1^M, \hat{x}_1^{i-1}) = \frac{w_M^{(i)}(y_1^M, \hat{x}_1^{i-1}|0)}{w_M^{(i)}(y_1^M, \hat{x}_1^{i-1}|1)} \tag{3}$$

where ${}^{(i)}_{M}(y_1^M, \hat{x}_1^{i-1}|\gamma)$ is the probability of noise that γ is 0 or 1. The decision is

$$\hat{x}_i = \begin{cases} x_i, & i \in A^C \\ h_i(y_1^M, \hat{X}_1^{i-1}), & i \in A \end{cases}$$

$$(i=1,2,3,\ldots,M) \tag{4}$$

and

$$h_i(y_1^M, \hat{x}_1^{i-1}) = \begin{cases} 0, & L_M^{(i)}(y_1^M, \hat{x}_1^{i-1}) \geq 1 \\ 1, & otherwise \end{cases} \tag{5}$$

Here, *hi* denotes the decision functions transmitted to all subsequent decision elements (DEs). The LR computation derived from recursive formulas is presented as follows:

$$L_M^{(2i-1)}(y_1^M, \hat{x}_1^{2i-2}) = f(L_{M/2}^{(i)}(y_1^{M/2}, \hat{x}_{1,0}^{2i-2} \oplus \hat{x}_{1,e}^{2i-2}), L_{M/2}^{(i)}(y_{M/2+1}^{M}, \hat{x}_{1,e}^{2i-2})) \tag{6}$$

$$L_M^{(2i)}(y_1^M, \hat{x}_1^{2i-1}) = g(L_{M/2}^{(i)}(y_1^{M/2}, \hat{x}_{1,0}^{2i-2} \oplus \hat{x}_{1,e}^{2i-2}), L_{M/2}^{(i)}(y_{M/2+1}^{M}, \hat{x}_{1,e}^{2i-2}), \hat{x}_{2i-1}) \tag{7}$$

f and *g* are defined as:

$$f(a,b) = \frac{1+ab}{a+b} \tag{8}$$

$$g(a,b,\hat{x}_{sum}) = a^{1-2\hat{x}_{Sum}}b \tag{9}$$

a, *b*, and $\hat{x}sum$ are defined as follows:

$$a = L_{M/2}^{(i)}(y_1^{M/2}, \hat{x}_{1,0}^{2i-2} \oplus \hat{x}_{1,e}^{2i-2}) \tag{10}$$

$$b = L_{M/2}^{(i)}(y_{M/2+1}^{M}, \hat{x}_{1,e}^{2i-2}) \tag{11}$$

$$\hat{x}_{Sum} = \hat{x}_{2i-1} \tag{12}$$

The SC decoder can be represented as a code tree to achieve low complexity. However, the decoding path obtained by the SC decoder may not be the most efficient [29]. On the other hand, the second type of polar decoding is called Successive Cancellation List (SCL). Using SCL significantly boosts the error-correction ability of SC for medium code lengths, particularly when paired with a CRC [30]. The aforementioned technique has served as a primary reference in evaluating error-correction performance within the realm of 5G technology [31]. The SCL decoder bifurcates the decoding pathway into two routes during the decoding of an information bit. As each division doubles the quantity of pathways to be evaluated, it is necessary to prune them, with the maximum permissible number of paths being the designated list size L [32].

IV. Proposed Approach

In this section, the proposed approach will be described, as shown in Fig. 2. In this work, the image stego design based on the NR-DCSK communication system is introduced. Both the cover and secret image convert to stream bits; after that, the embedding operation is applied using 1-LSB, where the LSB is the simplest method of inserting secret bits without influence on frame quality. The last bit in each pixel is replaced by stream bits of the secret image, as shown in Fig. 3 for the embedding operation.

After that, image steganography uses the NR polar code to transmit secret data over a wireless channel. This coding represents a concatenated multistage approach to error correction, where a CRC is appended to the vector data. The interleaving stage then begins with polarizing, which involves partitioning the polar code channels into high and low reliability. The reliable channels transmit data, while frozen bits assign fixed values to unreliable data. In this study, DCSK is used instead of regular modulation, which uses chaotic signals instead of sinusoidal carriers. This modulation offers a wide spectrum range due to chaotic features based on SF, allowing a link between the transmitter and receiver without the necessity for a synchronous connection. Fig. 4 depicts the transmitter and receiver blocks of the DCSK system. In this study, the chaos signal generated by the logistic map, which is a one-dimensional chaotic discrete map model frequently employed because it has a simple structure. On the other hand, the duration of DCSK symbols is partitioned into two equal time intervals; during the first interval, the reference chaotic sequence is communicated, while the identical or inverted version of the reference sequence is conveyed in the second interval, respectively. The DCSK modulation represents each bit using two equal-length chaotic segments.

The DCSK transmitter signal S_{i,κ_DCSK} for the initial input data is defined by equation (13):

$$S_{i,k\_DCSK} = \begin{cases} a_{i,k}, & k = 1,\ldots,\beta \\ (2x_i - 1)a_{i,k-\beta} & k = \beta+1,..,2\beta \end{cases} \tag{13}$$

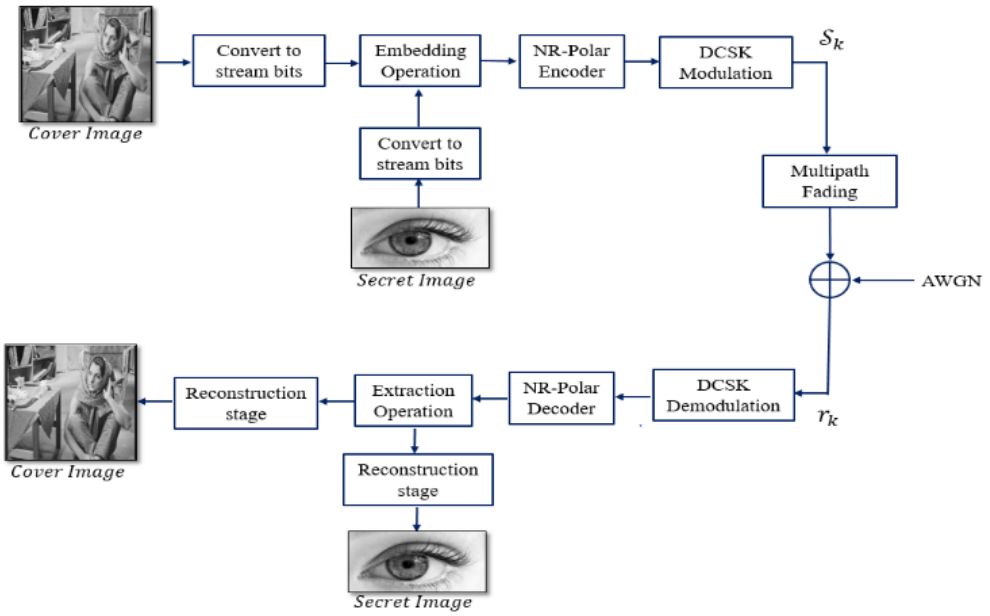

Fig. 2. General scheme for stego transmission system based on NR-DCSK.

Here, 2β denotes the spreading factor, x_i denotes the i^{th} transmitted bit, $x_i \in (0,1)$, and $a_{i,k}$ represent the k^{th} chaotic chip. At the receiver, the correlator's output Z_i is represented as:

$$Z_i = \sum_{k=\beta+1}^{2\beta} y_{i,k} y_{i,k+\beta} \tag{14}$$

where decoding transmitted bits involve correlating the received sequence $y_{i,k}$ with its delayed version $y_{i,k+\beta}$.
In this situation, where *rk* represents the received sequence, the polar decoder directly associates the correlator's output, thereby obviating the necessity to convey the decision variable via thresholding [33].

The AWGN channel, which incorporates Gaussian noise to simulate genuine wireless communication, will convey these frames. On the other hand, a more realistic scenario for wireless communications involves many pathways between transmitters and receivers. These pathways may be direct or produced by reflection, diffraction, and scattering. The collected signal represents a vector of multiple delayed signals, each characterized by distinct frequency, amplitude, and delay. The Rayleigh fading channel model is the most frequently employed for restricted bandwidth transmission across mobile and wireless channels, where all the frequency parts of the signal are weakened by the same amount when the flat fading channel is used. The received signal is obtained by transmitting the signal across a multipath Rayleigh fading channel and adding an AWGN signal $y(t) \in \mathcal{N}(0, N_0/2)$, which can be described as:

$$y_{i,k\_DCSK} = \sum_{\ell=1}^{\iota} \lambda_\ell S_{i,k-\tau_\ell} + \varsigma_k \tag{15}$$

where ι denotes the total number of pathways, while τ_ℓ and λ_ℓ represent the ℓ^{th} delay and coefficient of the channel, respectively. The symbol ς_k denotes the broadband AWGN wave characterized by a mean value of zero and a power spectral density of No/2. Random variables characterized by distinct Rayleigh probabilities are formulated to constitute the channel parameters λ_ℓ [34].

In the receiver, DCSK demodulation extracts the transmitted bits by correlating the received signal. The modulation block in this system transmits the reference chaotic signal during the initial segment of each symbol duration. In the latter segment of the symbolic time frame, the chaotic signal is either replicated or altered, depending on whether the data bit is one or zero.

Following this, LLR utilizes the SCL decoding algorithm with a list size (L) of 8 to retrieve the secret bits from the stego cover. The SCL decoder bifurcates the decoding pathway into two routes during the decoding of an information bit. As each division doubles the quantity of pathways to be evaluated, it is necessary to prune them, with the maximum permissible number of paths being the designated list size L.

V. Results & Discussion

This section discusses the design's performance evaluation by examining the results obtained from its execution in MATLAB R2021b. Barbara, Cameraman, and Lena are the basic grayscale images utilized to illustrate the system results. Each is in PNG format with a resolution of 256×256 pixels in steganography. Conversely, medical, eye, and flower JPGs with a resolution of 128×64 are utilized as concealed images. Several factors can measure the effectiveness of image transmission over a channel, such as the Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Entropy, Normalized Cross Correlation (NCC), and Bit Error Rate (BER). The MSE and PSNR are important metrics for evaluating the quality of image frames, where the MSE is the average of the squared errors of the differences between the original and extracted frames, while the PSNR is the signal

quality difference at the receiver. These parameters can be properly represented in the following equations:

$$MSE = \frac{1}{w \times h} \sum_{i=1}^{w} \sum_{j=1}^{h} (\quad p(i,j) - p^{'}(i,j))^2 \tag{16}$$

$$PSNR = 10 \times \log_{10} \frac{MAX^2}{MSE} \tag{17}$$

Let p represent the original frame and $p^{`}$ denote the steganography frame. Variables w and h denote the frame's width and height, respectively, while *MAX* signifies that the maximum pixel value is 255 [35]. On the other hand, NCC represents a tool that quantifies the degree of convergence between the original frame and its extracted counterpart at the receiver, providing a direct assessment of the proposed algorithm's efficacy. The most efficient algorithms generate images with correlation ratios closer to unity, where Equation (18) provides the description for the NCC mathematical model:

$$NC = \frac{\sum_i \sum_j c(i,j) c^{'}(i,j)}{\sum_i \sum_j [c(i,j)]^2} \tag{18}$$

where c and $c^{`}$ act as the image before and after image transmission [36]. Likewise, Information entropy is a critical security factor. It evaluates the randomness of the receiver's frame, targeting an optimal entropy value of 8. The parameter is delineated in Equation (19):

$$E(s) = -\sum_{i=1}^{n} P(c_i) \log_2 P(c_i) \tag{19}$$

Let s represent the collection of symbols, $P(c_i)$ denotes the probability, and n indicates the number of symbols [37]. Figs. 5 and 6 show the received stego and extracted images with coded and uncoded designs for SNR (10, 14, 18, and 24), respectively, where the NR-DCSK design improves the resistance against Rayleigh fading and noise over the AWGN channel. Table I denotes the results of the cover and secret extracted images with various parameters of different images.

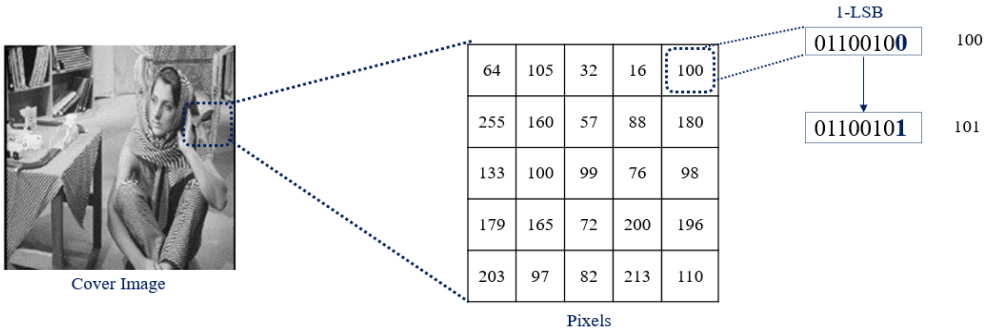

Fig. 3. 1-LSB Embedding process.

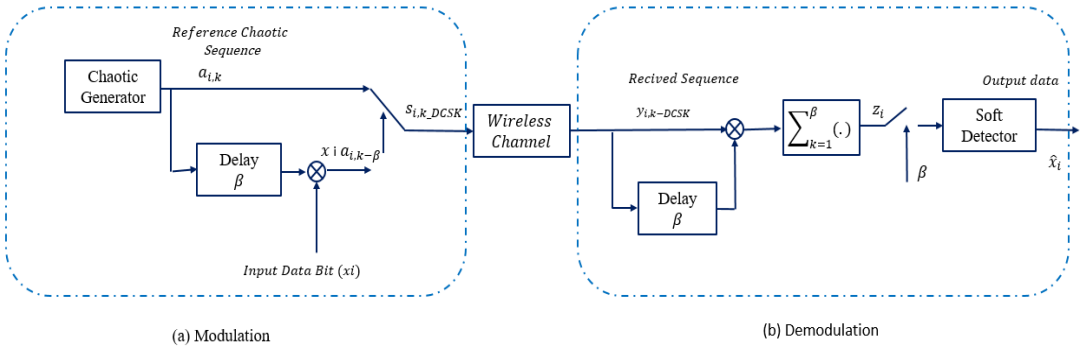

Fig. 4. DCSK modulation and demodulation system.

TABLE I

MEASUREMENTS OF EXTRACTED AND STEGO OVER AN AWGN AND RAYLEIGH CHANNEL AT DIFFERENT SNRS.

Standard Images	SNR(dB)	Cover image metrics				Secret image metrics			
		MSE	PSNR	NCC	Entropy	MSE	PSNR	NCC	Entropy
Barbara & Eye	10	1081.5	10.8809	0.22725	7.8902	1562.144	11.8635	0.2114	7.8624
	14	574.9109	17.2279	0.238	7.7619	329.5501	20.3995	0.6766	7.6019
	18	75.7990	27.5315	0.95112	7.3565	4.6391	29.9332	0.9255	7.2630
	24	0.9254	40.6608	0.9823	7.2895	0.1566	57.3219	0.9928	7.2036
Cameraman & Medical	10	995.78	10.9029	0.24619	7.7833	1625.441	12.4960	0.2328	7.9277
	14	877.1103	19.2192	0.58842	7.6733	551.2276	22.9533	0.6859	7.6368
	18	69.9979	30.4733	0.9877	7.2177	2.9857	29.0662	0.9670	7.3323
	24	1.3960	42.9243	0.9974	7.2060	0.0954	50.2482	0.9484	7.2047
Lena & Flower	10	1293.5	11.7693	0.2372	7.6911	1596.8	14.8823	0.2938	7.9041
	14	623.5913	19.1876	0.62099	7.4284	365.8491	21,4389	0.7644	7.5220
	18	70.3227	29.0140	0.95397	7.2996	3.5511	31.3921	0.9729	7.3662
	24	1.2031	44.9762	0.9933	7.2798	0.0863	54.2791	0.9217	7.2583

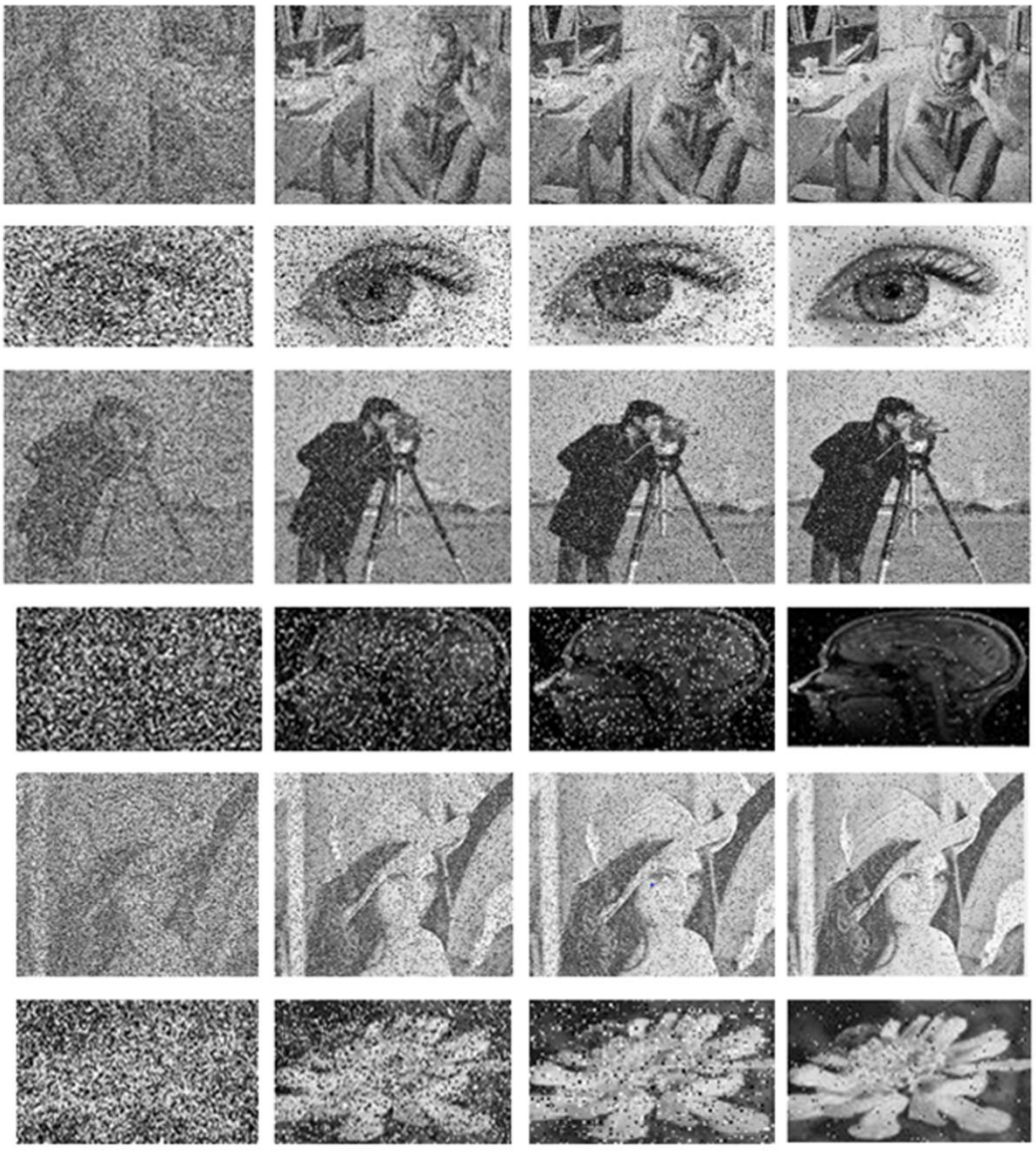

Fig. 5. Received stego and extracted images without NR-DCSK design.

Fig. 6. Received stego and extracted images with NR-DCSK design.

Finally, BER is an essential measure in digital communication systems, assessing the ratio of erroneously received bits to the total bits transmitted across the channel. Several factors can contribute to the error rates encountered during the transmission of frames over wireless channels. These factors include interference, attenuation, multipath propagation, and malicious actors. This study utilizes the NR-Polar Code based on the DCSK method to enhance the BER and improve the security of transmitted frames. Fig. 7 illustrates the performance of the BER design with varying SF over the AWGN channel at (43/180) of the Code Word (CW). It shows that the gain of this design reaches 8 dB at 32 SF over the AWGN channel, where the gain indicates the improvement in SNR between the BER performance with our design and without it. This shows that the Polar Code based on DCSK (PCDCSK) exceeds other techniques, where the broad bandwidth protects the secret data from loss due to the wireless channel's effectiveness. Additionally, Fig. 8 depicts the BER across various CWs at 32 SF, demonstrating that a higher code rate results in improved performance compared to other code rates. On the other hand, Fig. 9 represents the combined effect of Rayleigh fading and AWGN channel on the received stego images, where the gain of the BER reaches approximately 4 dB. Rayleigh fading is one of wireless fading through receiving the signal by multipaths due to various factors such as reflection, diffraction, and scattering over communication channels, which leads to delay and attenuation of the signal as well as loss of transmitted information. The power gains and time delays of the three-path fading channels are established as ($\alpha1 = \alpha2 = \alpha3 = 1/3$) and ($\tau1 = 0$, $\tau2 = 1$, $\tau3 = 2$), respectively.

Fig. 10 shows the BER with different CWs of the stego received image over the effect of fading. Finally, Fig. 11 demonstrates that the PSNR of this design is better than other designs without coding with different SFs, where it reached 80.2750 dB at 26 dB SNR with a 32 SF. Fig. 12 compares the BER performance of our proposal and the OFDM design [38] over AWGN and Rayleigh channels. The simulation results demonstrated that the PCDCSK, which used hybrid techniques

of DCSK and NR-polar code, performed better than other outcomes; hence, our design provides a gain of approximately 15 dB in BER performance over multipath fading compared to the OFDM-based steganography design. Additionally, our proposal provided a 5 dB improvement over the AWGN channel compared to the OFDM design.

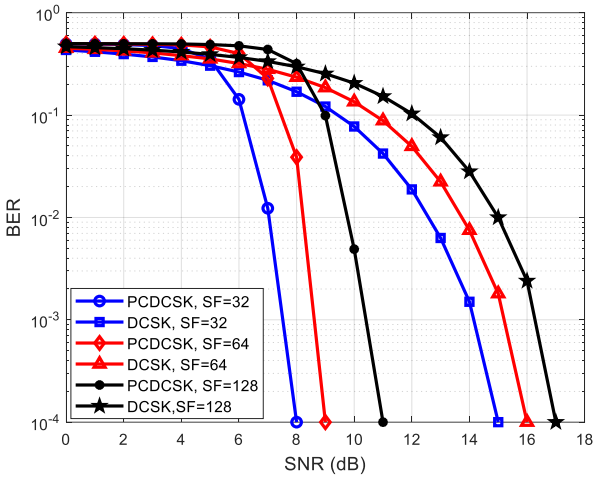

Fig. 7. BER performance of coded and uncoded stego designs over the AWGN channel.

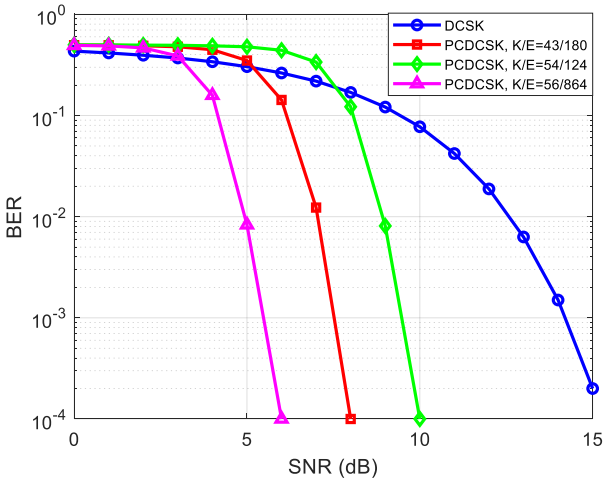

Fig. 8. BER performance of various CWs over the AWGN channel.

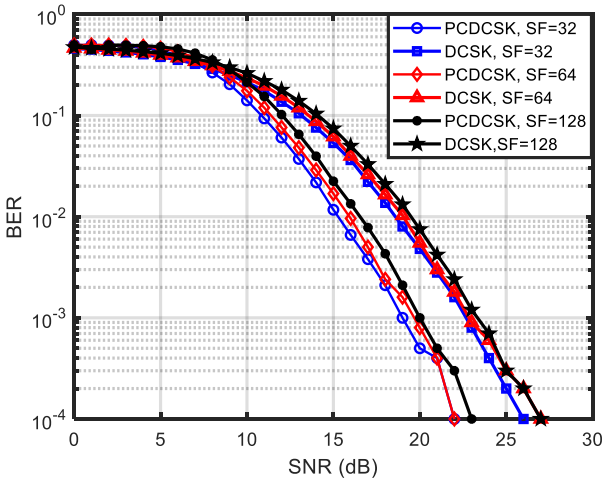

Fig. 9. BER performance of coded and uncoded stego designs over the AWGN and Rayleigh channel.

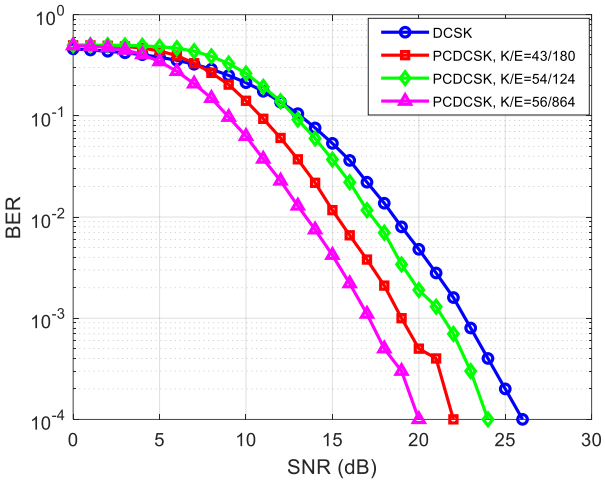

Fig. 10. BER performance of various CWs over the AWGN and Rayleigh channel.

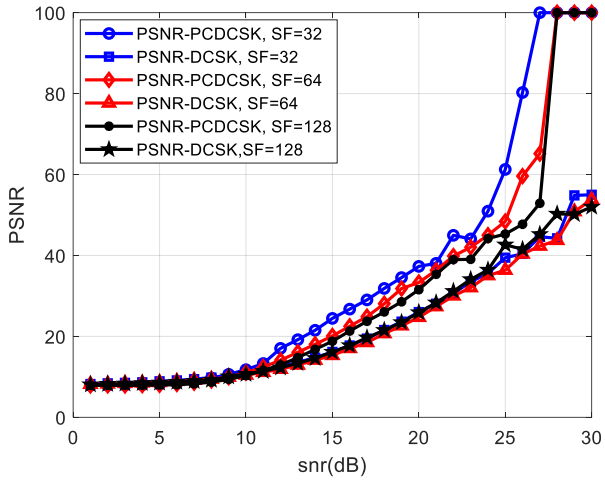

Fig. 11. PSNR performance of coded and uncoded over the AWGN and Rayleigh channel.

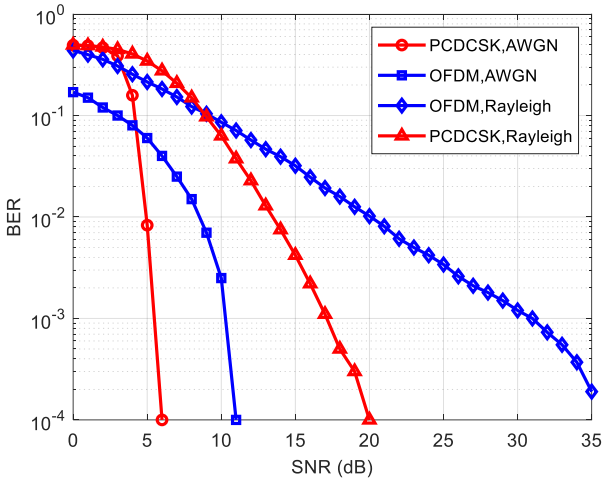

Fig. 12. BER performance of PCDCSK versus OFDM design.

VI. CONCLUSION

In this work, an efficient design of image steganography is introduced based on the NR-Polar code, which is characterized by low complexity and efficient performance. In this design, traditional modulation is replaced with DCSK, which is immune to fading and intruders. The secret image is inserted into the stego image using the LSB embedding operation; after that, the NR-PCDCSK is applied, where this design is transmitted over AWGN and Rayleigh fading channels. At the receiver, the SCL decoder is implemented to extract the cover image with effective error correction. The test evaluations have proven that this design exceeds others, where the PSNR reaches an efficient value of 26 dB SNR. Furthermore, the BER shows a 4 dB gain over the multipath fading channel. This work incorporates the secure image of steganography with a reliable channel coding system based on spread spectrum techniques to protect the secret image from attackers and the fading effect. In the future, we intend to develop this work by testing the suggested design over real communication channels, such as video streaming. Moreover, a comprehensive analysis based on machine learning against different attacks will be executed.

REFERENCES

[1] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," Arch. Computer. Methods Eng., vol. 27, no. 1, pp. 15–43, 2020.

[2] J. Wang, X. Jia, X. Kang, and Y.-Q. Shi, "A cover selection HEVC video steganography based on intra-prediction mode," IEEE Access, vol. 7, pp. 119393–119402, 2019.

[3] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," Health Technol. (Berl.), vol. 12, no. 1, pp. 9–31, 2022.

[4] X. Wang, X. Wang, B. Ma, Q. Li, and Y.-Q. Shi, "High precision error prediction algorithm based on ridge regression predictor for reversible data hiding," IEEE Signal Process. Lett. vol. 28, pp. 1125–1129, 2021.

[5] A. Bhardwaj, V.S. Verma, and R.K. Jha, "Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform", Multimedia Tools and Applications, Vol. 77, No. 15, pp. 19659- 19678, 2018.

[6] M. A. Hajjaji, M. Gafsi, A. Ben Abdelali, and A. Mtibaa, "FPGA implementation of digital images watermarking system based on discrete Haar wavelet transform," Secur. Commun. Netw, vol. 2019, pp. 1–17, 2019.

[7] A. Graell I Amat and L. Schmalen, Forward error correction for optical transponders. Springer Handbook of Optical Networks, 2020.

[8] C. Valerio and I. Condo, "Design of polar codes in 5G new radio," IEEE Communications Surveys & Tutorials, vol. 23, pp. 29–40, 2020.

[9] J. Del Olmo Alòs and J. R. Fonollosa, "Polar coding for confidential broadcasting," Entropy (Basel), vol. 22, no. 2, p. 149, 2020.

[10] J. Feng, W. Li, J. Xiao, J. Han, H. Li, L. Huang, Y. Zheng, "Carrier phase estimation for 32-QAM optical systems using quasi-QPSK-partitioning algorithm," IEEE Photonics Technol. Lett., vol. 28, no. 1, pp. 75–78, 2016.

[11] L. De La Fraga, B. Martínez, and E. T. Cuautle, "Echo state network implementation for chaotic timeseries prediction," Microprocess. Microsyst, vol. 103, pp. 1–7, 2023.

[12] E. Tlelo-Cuautle, L. G. De La Fraga, O. Guillén-Fernández, and A. Silva-Juárez, "Optimization of Integer/Fractional Order Chaotic Systems by Metaheuristics and Their Electronic Realization". Boca Raton, FL, USA: CRC Press, 2021.

[13] P. K. Vitthaladevuni and M.-S. Alouini, "Effect of imperfect phase and timing synchronization on the error rate performance of PSK modulations," in Proceedings IEEE 56th Vehicular Technology Conference, 2002.

[14] A. Banerjee and B. Jana, "A robust reversible data hiding scheme for color image using reed-Solomon code," Multimed. Tools Appl., vol. 78, no. 17, pp. 24903–24922, 2019.

[15] W. Lu, J. Zhang, X. Zhao, W. Zhang, and J. Huang, "Secure Robust JPEG Steganography Based on AutoEncoder With Adaptive BCH Encoding," IEEE Trans. Circuits Syst. Video Technol., vol. 31, no. 7, pp. 2909–2922, 2021.

[16] Y. Wang, M. Tang, and Z. Wang, "High-capacity adaptive steganography based on LSB and Hamming code," Optik (Stuttg.), vol. 213, no. 164685, p. 164685, 2020.

[17] K. Ying, R. Wang, Y. Lin, and D. Yan, "Adaptive audio steganography based on improved syndrome-trellis codes," IEEE Access, vol. 9, pp. 11705–11715, 2021.

[18] J. Hao, L. Liu, and W. Chen, "Performance of Polar-Coded 3D Image Transmission over Fading Channel," Mathematical Problems in Engineering, vol. 2020, 2020.

[19] F. Alharbi, "Steganography performance over AWGN channel," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 8, 2019.

[20] W. Li, W. Zhang, L. Li, H. Zhou, and N. Yu, "Designing near-optimal steganographic codes in practice based on polar codes," IEEE Trans. Commun., vol. 68, no. 7, pp. 3948–3962, 2020.

[21] Q. Yao, K. Zeng, W. Zhang, and K. Chen, "Reliable Robust Adaptive Steganographic Coding Based on Nested Polar Codes," IEEE Transactions on Signal Processing, 2024.

[22] Q. Guan, K. Chen, W. Lu, W. Zhang, and N. Yu, "Non-Binary Polar Codes for Steganography," IEEE Trans. Dependable Secure Comput., pp. 1–18, 2025.

[23] H. Hadi, A. Sameer, and O. Gazi, "The Research and Design of Multi Relays in Cooperative Communication System Based on Polar Codes". 2021.

[24] M. Mondelli, S. H. Hassani, and R. Urbanke, "Construction of polar codes with sublinear complexity," in IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, June 2017.

[25] C. Valerio and I. Condo, "Design of polar codes in 5G new radio," IEEE Communications Surveys & Tutorials, vol. 23, pp. 29–40, 2020.

[26] K. Niu, Y. Li, and W. Wu, "Polar codes: Analysis and construction based on polar spectrum," arXiv [cs.IT], 2019.

[27] A. Balatsoukas-Stimming, A. J. Raymond, W. J. Gross, and A. Burg, "Hardware architecture for list successive cancellation decoding of polar codes," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 61, no. 8, pp. 609–613, Aug. 2014.

[28] A. Ç. Arli and O. Gazi, "A survey on belief propagation decoding of polar codes," China Commun., vol. 18, no. 8, pp. 133–168, 2021.

[29] A. J. Al-Askery, F. S. Hasan, and Y. A. Yassin, "Polar-coded differential/quadrature chaos shift keying communication systems for underwater acoustic channels," Telecom, vol. 5, no. 2, pp. 476–486, 2024.

[30] I. Sagitov, C. Pillet, A. Balatsoukas-Stimming, and P. Giard, "Generalized restart mechanism for successive-cancellation flip decoding of polar codes," arXiv [cs.IT], 2025.

[31] V. Miloslavskaya, Y. Li, and B. Vucetic, "Frozen Set Design for Precoded Polar Codes," IEEE Trans. Commun., pp. 1–1, 2024.

[32] M. Vlad-Florin and J. Rowshan, "On the Closed-form Weight Enumeration of Polar Codes: 1.5d-weight Codewords," IEEE Transactions on Communications, 2024.

[33] A. J. Al-Askery, A. K. Al-Ali, F. S. Hasan, "Performance Analysis of NR-DCSK Based Copper Cable Model for G.fast Communication," Telecom, vol. 6, no. 1, 2025.

[34] A. J. Al-Askery, F. S. Hasan, and A. A. Thabit, "Investigating the performance of coded GSIM DCSK communication systems over multipath Rayleigh fading channel," J. Commun. Softw. Syst., vol. 20, no. 4, pp. 298–306, 2024.

[35] A. Ouannas and M. M. Al-Sawalha, "On inverse full state hybrid projective synchronization of chaotic dynamical systems in discrete-time," Int. J. Dyn. Contr., vol. 5, no. 2, pp. 252–258, 2017.

[36] G. Maji, S. Mandal, and S. Sen, "Cover independent image steganography in spatial domain using higher order pixel bits," Multimed. Tools Appl., vol. 80, no. 10, pp. 15977–16006, 2021.

[37] J. Khan and J. Sher, "Chaos-based efficient selective image encryption," Multidimensional Systems and Signal Processing, vol. 30, pp. 943–961, 2019.

[38] A. A. Eyssa, F. E. Abdelsamie, and A. E. Abdelnaiem, "An efficient image steganography approach over wireless communication system," Wirel. Pers. Commun., 2020.

Noor Dheyaa Majeed was born in Baghdad, Iraq, in 1989. She received her B.Sc. degree in Electrical Engineering in 2014 and her M.Sc. degree in Electronics and Communication Engineering in 2021, from the Middle Technical University, Electrical Engineering Technical College, Baghdad, Iraq. She is currently pursuing a PhD. in Communication Engineering at the department of Computer Engineering, Middle Technical University. Her research interests include wireless communication, polar code, DCSK, steganography, and secret image.

Ali Jaber Al-Askery is a professor at the Technical Engineering College of Artificial Intelligence–Middle Technical University in Baghdad, Iraq. He obtained the B.Sc. and M.Sc. degrees in Electrical Engineering from Al-Mustansiriyah University, Baghdad, Iraq, in 2001 and 2004, respectively. He obtained his PhD from the School of Electrical and Electronics Engineering at Newcastle University, Newcastle Upon Tyne, U.K. His research concentrates on wireless communications, wired communications, OFDM systems, coded systems and receiver design.

Fadhil Sahib Hasan was born in Baghdad, Iraq, in 1978. He obtained his B.Sc. in Electrical Engineering in 2000 and his M.Sc. in Electronics and Communication Engineering in 2003, both from Mustansiriyah University, Iraq. He obtained his PhD. in Electronics and Communication Engineering from Basrah University, Iraq, in 2013. In 2005, he became a member of the Faculty of Engineering at Mustansiriyah University in Baghdad. His recent research endeavors encompass wireless communication systems, multicarrier systems, wavelet-based OFDM, MIMO systems, speech signal processing, chaotic modulation, and communication systems utilizing FPGA and Xilinx System Generator. He has been a lecturer at Mustansiriyah University in Iraq since 2022.