Alkadhim Journal for Computer Science, Vol. 02, No. 4 (2024)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

Transmission of High Data Rate Signals over Low-Frequency Passbands Using (DSSS-BPSK) Technique

[1]Khduer Essam Ahmed, [2]Hadi R. Ali, [3]Hayder Ayyed Naser* and [4]Mohammed Zorah

[1,2,3,4] Imam AlKadhim University College, Department of Computer Techniques Engineering, Baghdad, Iraq

Article information

Article history:
Received: November, 02, 2024
Accepted: December, 01, 2024
Available online: December, 25, 2024

Keywords:
Direct Sequence Spread Spectrum,
DSSS,
High Data Rate Transmission,
Low-Frequency Passbands,
Encryption Complexity,
Binary Phase Shift Keying

****Corresponding Author:***
Hayder Ayyed Naser
hayder.a.naser@gmail.com

DOI:
https://doi.org/10.61710/kjcs.v2i4.85

Abstract

This study presents an enhancement to the Direct Sequence Spread Spectrum (DSSS) algorithm aimed at transmitting high data rate signals over low-frequency passbands. By utilizing a random number to generate a new encryption key, the complexity of both encryption and decryption processes is significantly increased. The original signal undergoes multiplication with a spreading code, resulting in a random matrix that obscures the original data and enhances security. The research employs Binary Phase Shift Keying (BPSK) modulation to effectively transmit the spread signal, optimizing bandwidth utilization and mitigating channel impairments. Simulation results conducted using MATLAB demonstrate that the proposed DSSS method achieves low Bit Error Rates (BER) under various conditions, confirming its robustness against interference. Furthermore, the findings indicate that the combination of high data rate transmission and low-frequency passbands using DSSS has promising applications in diverse fields such as industrial automation, remote sensing, and military communications. Overall, this research contributes to advancing secure and efficient communication systems by leveraging DSSS techniques.

1. Introduction and literature review

High data rate transmission over low-frequency passbands is valuable in wireless communication systems, particularly in scenarios where long-range coverage and penetration through obstacles are essential. Examples include long-range internet of things (IoT) [1], Free space optical (FSO) communication system [2], and wide-area chaotic systems [3,4]. Multiple methods for disseminating information signals, which can be employed to generate targeted signals. These methods encompass: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Time Hopping Spread Spectrum (THSS) [5,6]. The DSSS technique represents one of the developed spread spectrum techniques to increase resistance against interference and enhance data security. By utilizing a distinct code, the DSSS system expands the baseband signal, which has been digitally modulated with information. This system boasts easy implementation and facilitates high-speed data transmission [7]. Spread spectrum communication, in comparison to narrowband communication, exhibits a robust resistance to interference and can effectively ensure the reliability of the communication system [8]. As the spreading factor increases, the Bit Error Rate (BER) performance improves [9]. DSSS has various applications in our daily lives, enabling robust wireless communication [1,10], high data security [11,12], improved minimum detectable signal, extended transmission distance [13] and jamming attacks prevent [14]. Various types of codes can be used for spreading and encoding data, the choice of the code depends on the specific requirements, system constraints, and the trade-offs between complexity, performance, and application-specific considerations [15]. DSSS codes of a signal have different effects on the compensation of nonlinear signal distortions and external interference [16,17]. The commonly used modulator in DSSS systems is Binary Phase Shift Keying (BPSK) due to its simplicity and robustness. BPSK is often suitable for applications with lower data rates and where power efficiency is a critical factor [18-20]. A secure communication system that combines chaos and (DS/SS) techniques are presented by [21]. A theoretical analysis of the principles and characteristics of the DSSS system, along with a comparison to another widely used technology, is provided by [5]. Detecting differential DSSS signals has been tested [22]. [23] proposed a technique for estimating the spreading code of non-periodic long-code DSSS (NPLC-DSSS) signals. To estimate delay and frequency offset for DSSS signals, [24] designed two discriminators. A Doppler frequency search strategy for DSSS signal acquisition was detailed by [25], while [26] proposed a fractal dimension estimation scheme for the DSSS frame preamble. A purely signal-processing based anomaly detector is developed for (DSSS) signals [27]. Multilocation radio signals are employed with (DSSS) to adapt Power Wireless Control Systems (PWCS) to mitigate existing narrow-band interference [28]. A multi-criteria synthesis approach for generating signals using (DSSS) in order to adapt Cognitive Radio Communication Systems (CRCS) to complex interference conditions are provided by [29]. [30] present several key results demonstrating the effectiveness of the 3DES system for secure data transmission using DSSS. The specific problem being addressed in this study is the challenge of transmitting high data rate signals over low-frequency passbands while ensuring robust security and reliability in wireless communication systems. As wireless technologies evolve, there is a growing need for efficient methods that can maintain high data integrity and security, especially in applications requiring long-range coverage and penetration through obstacles. The unique contribution of this study lies in its proposed enhancement to the DSSS algorithm. By integrating a random number generation process to create new encryption keys and employing mathematical operations, particularly multiplication, on the original signal, the study significantly increases the complexity of both encryption and decryption processes. This approach not only improves data security by obscuring the original information but also optimizes bandwidth utilization and mitigates channel impairments. Through simulations conducted using MATLAB, the research demonstrates that the enhanced DSSS method achieves low BER under various conditions, confirming its effectiveness against interference.

2. Methodology

The study involves encoding data sources using spread codes and subsequently modulating the resulting spread-spectrum signal with BPSK before transmission. The carrier frequency is set lower than the bandwidth occupied by the spread data to effectively modulate and shift the signal into the desired frequency range. On the receiving end, demodulation is performed using a locally generated replica of the pseudonoise (PN) sequence for synchronization.The research includes a simulation program that investigates various stages of DSSS processing with a focus on digital data comprising 30 bits. The data undergoes spreading using codes before being modulated with BPSK and transmitted. The received signal is demodulated and despread, allowing for comparison between received and transmitted data bits to calculate BER. Figure 1 illustrates the main steps in creating DSSS signals. The transmitter (Tx) performed the following processes: Generation of information signals, spreading process using BPSK modulation of the spread signal. The resulting spread signal, obtained by spreading the information signal, was then modulated with BPSK. At the receiving side (Rx), the reverse process takes place, which involves demodulation and dispreading. The demodulation process is applied to the received signal, followed by the dispreading process.

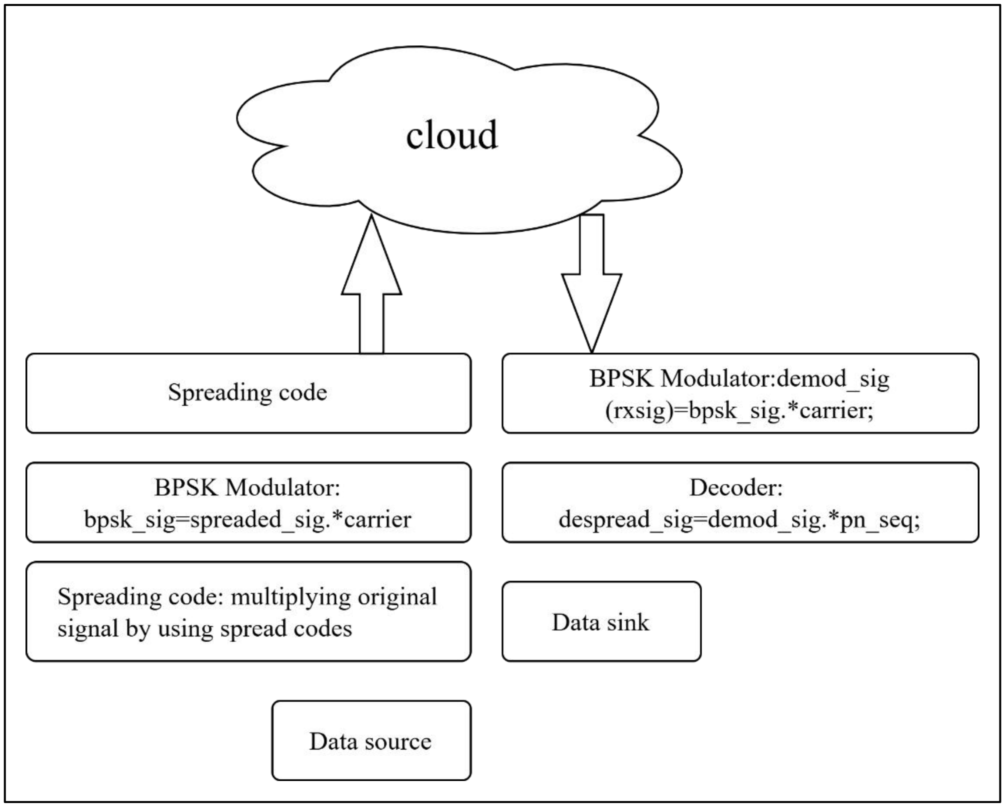


Figure1: The structure of the DSSS system: (a)Transmitting end (b) Receiving end.

To despread the Direct Sequence (DS) signal, it is multiplied (correlated) with a locally generated replica of the PN sequence. Conversely, a jammer, characterized by an incident power level J and a bandwidth of BJ, is spreaded in such a way that the power spectral density (SJ) at the output of the correlator matches the expression provided in equation (1) [15].

$$= \frac{\quad}{(\quad + \quad)} \qquad (1)$$

The given expression clearly illustrates that a narrowband jammer tends to be more effective in interfering with a direct sequence receiver compared to a wider bandwidth jammer [15].

3. Results and Discussions

3.1 DSSS Simulation Results on Channels

The processes of generating information signals, spreading the signal, and BPSK modulation of the spread signal are performed at the transmitter. The resulting spread signal, created by spreading the information signal, is then modulated using BPSK. Figure 2 illustrates key processes, including the encoding and decoding of original signals, as well as the analysis of spectral power densities under various conditions. Both BPSK and the power spectral density (PSD) are depicted.

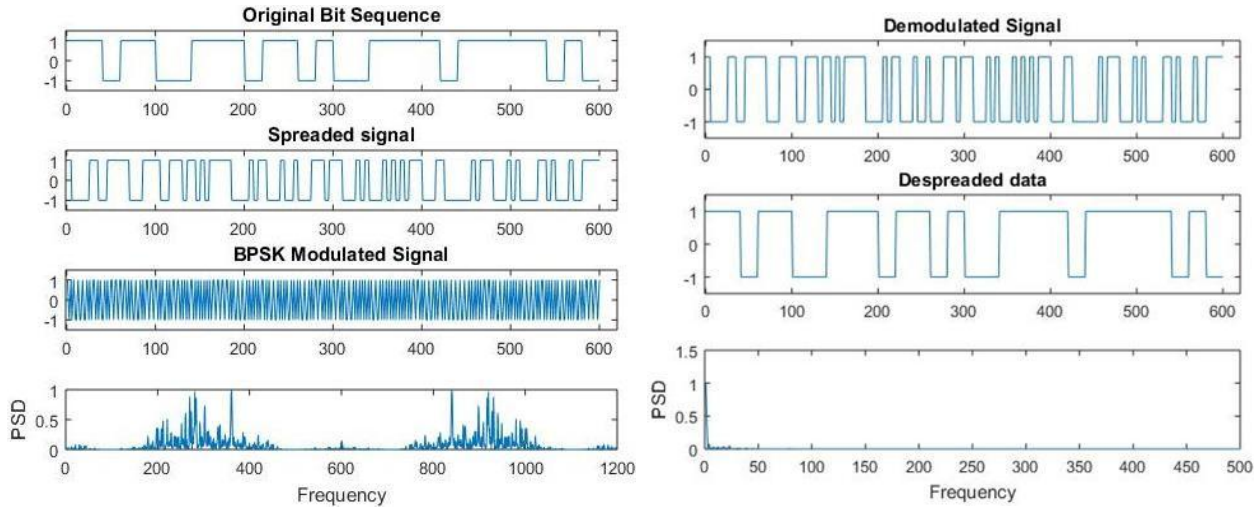
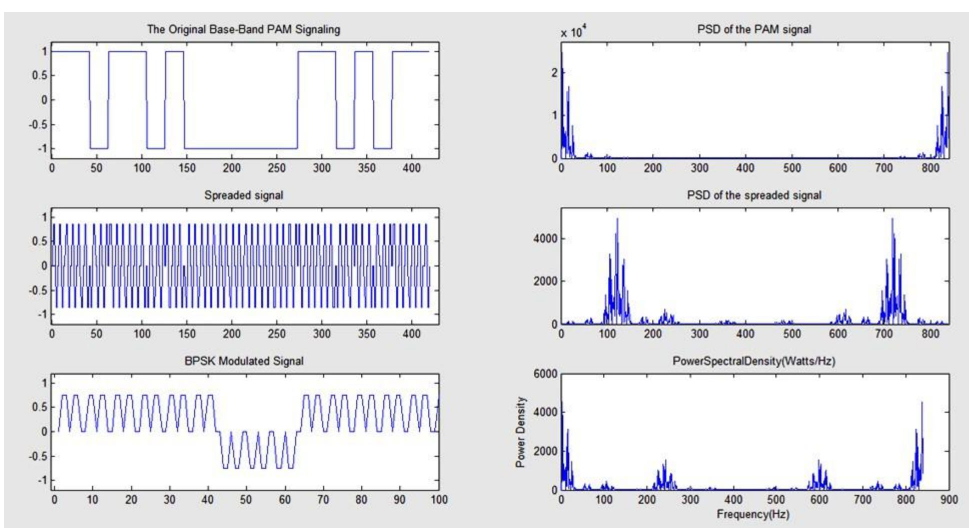


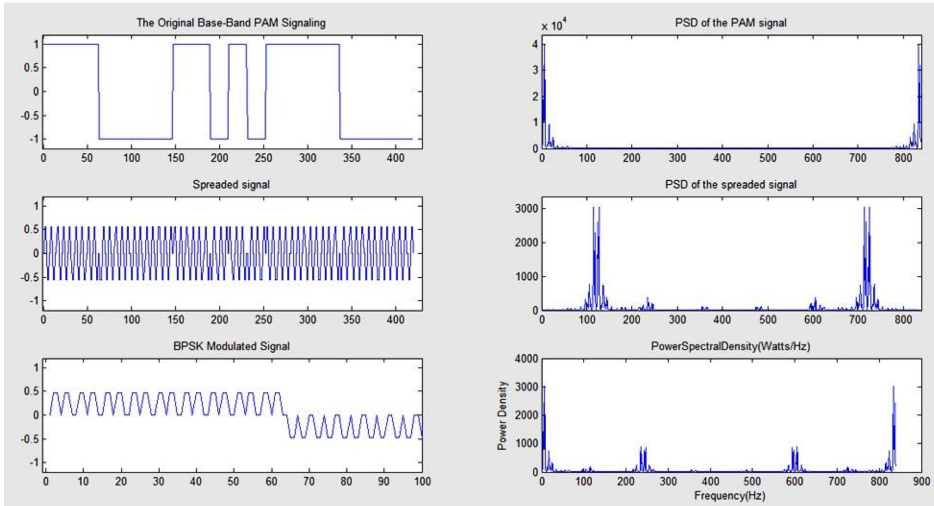
Figure 2. The encryption and decryption process using DSSS. It compares the original signal with its encrypted version, showing how one bit is spread across multiple bits in the processed signal, enhancing security.

Various mathematical operations applied to the spread signal were tested, each influencing security differently. Tests were conducted on several mathematical operations applied to the spreader signal values, which were encoded and decoded alongside the modulated values of the BPSK signal. Figure 3 illustrates the modification process, where the spreader signal function is multiplied by the carrier function to evaluate its impact on security. The original baseband pulse of amplitude modulation (PAM) signaling-such as audio, video, or image data is transmitted without modulation and then spread using the DSSS technique.

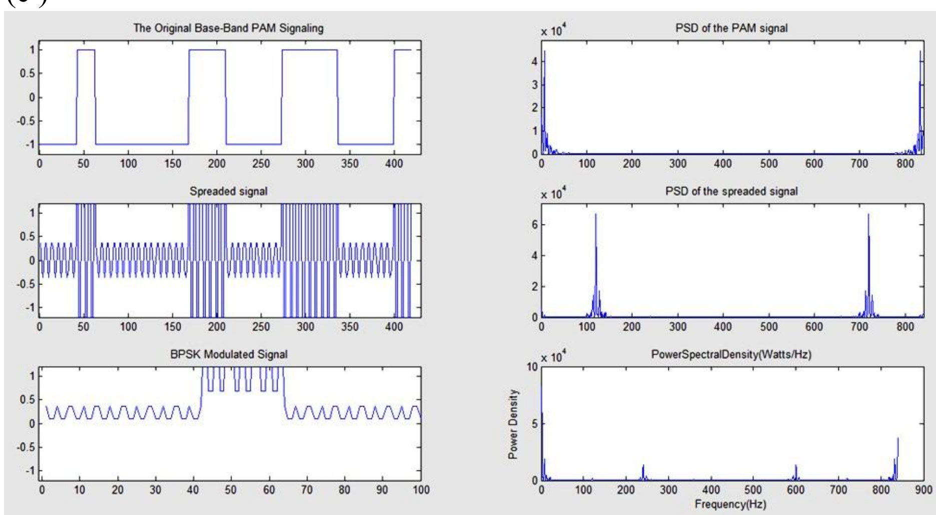
(a)



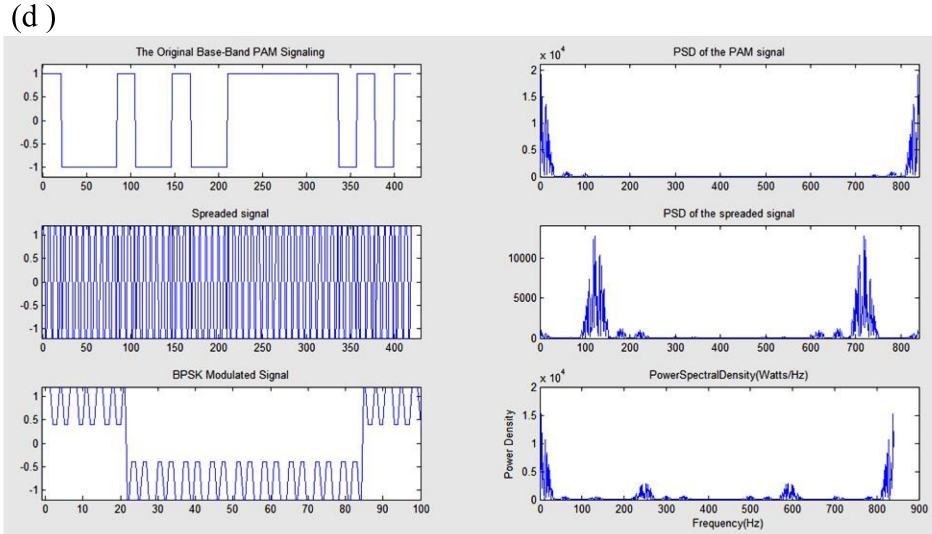
(b)


The Original Base-Band PAM Signaling
PSD of the PAM signal
Spreaded signal
PSD of the spreaded signal
BPSK Modulated Signal
PowerSpectralDensity(Watts/Hz)
Power Density
Frequency(Hz)

(c)


The Original Base-Band PAM Signaling
PSD of the PAM signal
Spreaded signal
PSD of the spreaded signal
BPSK Modulated Signal
PowerSpectralDensity(Watts/Hz)
Power Density
Frequency(Hz)

(d)


The Original Base-Band PAM Signaling
PSD of the PAM signal
Spreaded signal
PSD of the spreaded signal
BPSK Modulated Signal
PowerSpectralDensity(Watts/Hz)
Power Density
Frequency(Hz)

(e)

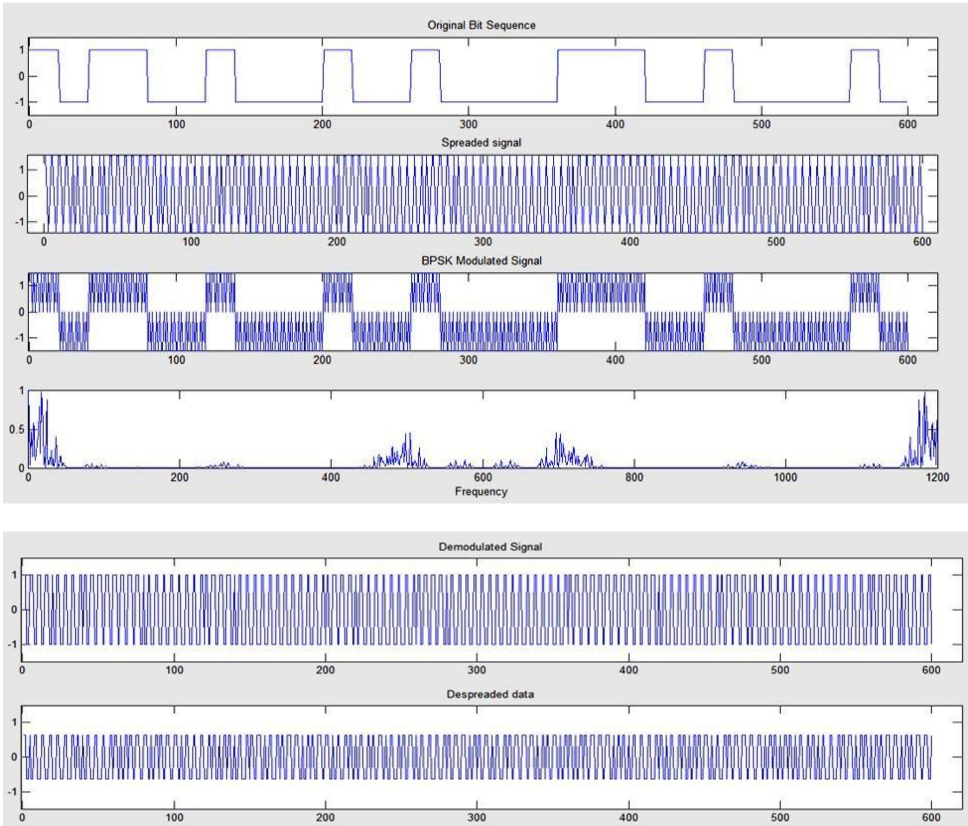


Figure 3. Modifications on the Spreader Signal Function. (a) multiply it by the carrier function, (b) the spreaded signal is multiply it by the cot function, (c) with the exp function, (d) with the tan function, (e) with the tan function.

Figure 3 demonstrates the effects of various mathematical operations applied to the spread signal, such as multiplication with different functions (e.g., carrier, cotangent, exponential). The results emphasize how these operations influence signal security. Some operations preserve identifiable features of the original signal, while others produce a more obscured output, offering better security. However, it is observed that the signal characteristics resulting from these calculations do not fully encode the image, as certain features of the image remain discernible. In Figure (3-e), the experiment stands out among prior tests for yielding a highly optimized modulated signal with significantly improved encryption quality. This improvement is attributed to the numerous adjustments made during the testing process. The spectral power under different conditions, as shown in this figure, reveals the impact of each encoding method on spread spectrum capacity. The original Pulse Amplitude Modulation (PAM) signal exhibits a smaller spread spectrum capacity due to lower noise levels, whereas BPSK-modulated signals display greater spectral power. This analysis underscores the effective utilization of bandwidth in DSSS while maintaining signal integrity.

Table 1 and Figure 4 summarize the encoding and decoding time results for the scenarios depicted in Figure 3. The results indicate that encoding and decoding times increase with higher encryption strength due to the increased complexity of the mathematical operations involved.

Table 1: Time coding of a DSSS-BPSK system

function	encoding Time (Sec)	decoding Time (Sec)
a	0.38147	0.0024951
b	0.3958	0.0025539
c	0.47225	0.0038208
d	0.55475	0.006727
e	0.46108	0030175

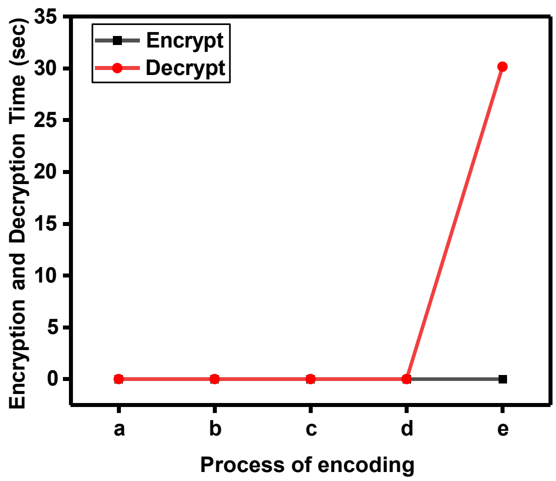


Figure 4. Time coding of a DSSS-BPSK system

Figure 5 displays the BER for different delay values in a DSSS-BPSK system. The Bit Error Rate performance was evaluated under varying delay values, confirming that increased delays improve noise immunity while maintaining low error rates. The results confirm that increasing delay values can enhance noise immunity and reduce interference, leading to lower BER percentages. This finding underscores the effectiveness of the proposed method in ensuring reliable data transmission under varying conditions. The BER in a DSSS-BPSK system can be affected by various factors, including the spreading code, delay values, channel conditions, and receiver design.

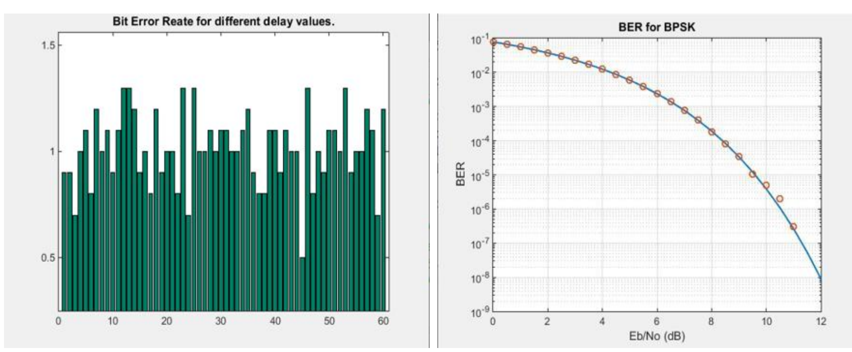


Figure (5): Bit Error Rate for different delay values and BPSK, respectively.

The study shows that DSSS successfully encrypts and decrypts signals, with the encrypted signal exhibiting high security. It also reports low BER across various conditions, indicating the method's resilience to data loss. BER is influenced by factors such as spreading code length, channel conditions, and delay values, with increased delay improving noise immunity. MATLAB simulations confirmed that DSSS enables efficient data transmission over low-frequency passbands, optimizing bandwidth usage and mitigating channel impairments. The results demonstrated superiority compared to similar studies, as shown in [30].

4. Conclusions

In this paper, high data rate signals over low-frequency passbands in a DSSS-BPSK system enable efficient spectrum utilization, enhanced robustness, improved security, and the potential for higher data rates. By integrating a random number generation process for key creation and applying multiplication in the encoding phase, encryption complexity is increased, making unauthorized access more difficult. BPSK modulation optimizes the transmission process, efficiently utilizing bandwidth and reducing the effects of channel impairments. Simulation results confirm that the proposed DSSS method achieves low Bit Error Rates (BER), enhancing its robustness under various conditions. The research highlights the importance of mathematical operations in improving signal security by obscuring original data characteristics. It also identifies practical applications for the enhanced DSSS approach in industrial automation, remote sensing, and military communications. Future research may focus on real-world implementation challenges and the exploration of alternative spreading codes to optimize performance in diverse communication scenarios. As technology evolves, these advancements can be leveraged to improve efficiency and security in data transmission.

References

[1] Naser, H. A., Ali, H. H., & Ali, H. R. (2023, February). Utilizing a High-Sensitive and Secure Communication System for Data Transmission. In *2023 Second International Conference on Advanced Computer Applications (ACA)* (pp. 1-5). IEEE.

[2] Lateef, A. T., Naser, H. A., & Kadhim, A. K. (2023, March). Comparing of the effect of changing weather factors on FSO communication system performance using iterative improvement technique. In AIP Conference Proceedings (Vol. 2591, No. 1). AIP Publishing.

[3] Naser, H. A. (2022). Design and Analysis of Radio Chaotic Circuit on Communication Network. Knowledge-Based Engineering and Sciences, 3(2), 44-51. https://doi.org/10.51526/kbes.2022.3.2.44-51

[4] Naser, H. A., & Mousa, S. K. (2020, May). Chaos Generation Utilizing Optical Feedback Technique with Modern Applications. In Journal of Physics: Conference Series (Vol. 1530, No. 1, p. 012137). IOP Publishing.

[5] Gao, Y. (2022, April). The analysis on the direct sequence spread spectrum communication system. In International Conference on Network Communication and Information Security (ICNCIS 2021) (Vol. 12175, pp. 69-74). SPIE.

[6] Patmanee, J., & Kanprachar, S. (2022). Performance of DSSS Signal Transmission with SCM over Low-Frequency MMF Passbands. ECTI Transactions on Electrical Engineering, Electronics, and Communications, 20(2), 242-255.

[7] Al-Rawi, M. (2020). Study of the tracking of FHSS signal over AWGN channel. *International Review of Applied Sciences and Engineering*.

[8] Yuan, F., Jia, Z. Y., & Cheng, E. (2020). Chirp-rate quasi-orthogonality based DSSS-CDMA system for underwater acoustic channel. Applied Acoustics, 161, 107163.

[9] Redd, B., & Rice, M. (2022). A Direct Sequence Spread Spectrum Solution to the Two-Antenna Problem. International Foundation for Telemetering.

[10] Kuznetsov, A., Onikiychuk, A., Peshkova, O., Gancarczyk, T., Warwas, K., & Ziubina, R. (2022). Direct spread spectrum technology for data hiding in audio. Sensors, 22(9), 3115.

[11] Reddy, B. S. K., & Goel, A. K. Spread Spectrum Sensing Techniques for Transformer Frequency Response Data. International Journal of Innovative Technology and Exploring Engineering (IJITEE).Vol.8 Issue-12, October 2019. P.p. 5203- 5210.

[12] Liu, F., Liu, J., & Feng, Y. (2021). Incremental-data stealth-transmission method in DSSS. Wireless Networks, 27, 2441-2449.

[13] Tabatabaefar, M., Ardakani, M. D., Karimian, R., & Tatu, S. O. (2021, January). A secure telecommunication link using spread spectrum technique for 5G applications. In 2021 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM) (pp. 29-30). IEEE.
[14] Navas, R. E., Cuppens, F., Cuppens, N. B., Toutain, L., & Papadopoulos, G. Z. (2021). Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming. Computer Networks, 187, 107751.
[15] Kaittan, K. H., & Mohammed, S. J. (2021). Implementing and designing a secure information system based on the DSSS gold sequence using MATLAB. Bulletin of Electrical Engineering and Informatics, 10(3), 1455-1463.
[16] Fedorenko, V., Samoylenko, I., Samoylenko, V., & Rachkov, V. (2022). Algorithms for distributing DSSS codes in industrial WSNs with real transmitters and narrow-band interference. AEU-International Journal of Electronics and Communications, 154, 154307].
[17] Lu, Z., & Jiao, Y. (2022). Efficiently All-Digital Code Tracking for Band-Limited DSSS Systems. IEEE Communications Letters].
[18] Jung, S., Im, G., Jung, D. H., Kim, P., Ryu, J. G., & Kang, J. (2022). Performance analysis of DSSS-and CSS-based physical layer for IoT transmission over LEO satellites. ETRI Journal, 44(4), 543-559.
[19] Rao, P. S., Lakshmi, N., & Geetanjali, V. (2019). Implementation of BPSK, DSSS and DQPSK Modulators and their Performance Comparison in VHDL". International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(6), 1713-1716.
[20] Xie, R., Wang, B., Qiu, W., Qiao, S., Zhu, W., Rui, Y., & Li, P. (2019, April). Joint code acquisition and Doppler shift estimation method for DSSS-MSK signal. In Tenth International Conference on Signal Processing Systems (Vol. 11071, pp. 73-81). SPIE.
[21] Xuan Quyen, N., Van Yem, V., & Manh Hoang, T. (2013). A chaos-based secure direct-sequence/spread-spectrum communication system. In Abstract and applied analysis (Vol. 2013, No. 1, p. 764341). Hindawi Publishing Corporation.
[22] Hartono, N. K., Putri, F. A., & Ananda, F. E. (2021). Simulasi Direct Sequence Spread Spectrum (DSSS) Pada Modulasi Binary Phase Shift Keying (BPSK). Spektral, 2(1), 45-49.
[23] X. Qiang and T. Zhang, "Estimation of spreading code in non-periodic long-code DSSS signal," 2021 sixth international conference on wireless communications, signal processing and networking (WiSPNET), pp. 162–165, Mar. 2021.
[24] W. Wang, Y. Wang, Y. Shen, and S. Wu, "Cell-Straddling Robust-Fast Cross-Correlation Mitigation via MMSE filter for DSSS Signals," IEEE Transactions on Aerospace and Electronic Systems, 2023.
[25] Y. He, X. Shi, Y. Wang, and Y. Shen, "Intelligent search strategy for Doppler frequency based on fuzzy logic in DSSS signal acquisition," IEEE Transactions on Aerospace and Electronic Systems, 2023.
[26] X. Li et al., "Fractal Dimension of DSSS Frame Preamble: Radiometric Feature for Wireless Device Identification," IEEE Transactions on Mobile Computing, 2023.
[27] Kochańska, I. (2021). A new direct-sequence spread spectrum signal detection method for underwater acoustic communications in shallow-water channel. Vibrations in Physical Systems, 32(1).
[28] Roy, D., Chaudhury, V., Tassie, C., Spooner, C., & Chowdhury, K. (2023, May). Icarus: Learning on iq and cycle frequencies for detecting anomalous rf underlay signals. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications (pp. 1-10). IEEE.
[29] Kirillov, S. N., & Lisnichuk, A. A. (2020, March). The Procedure of Multi-Criteria Synthesis of DSSS Radio Signals to Adapt Prospective Wireless Communication Systems to the Action of NarrowBand Interference. In *2020 Moscow Workshop on Electronic and Networking Technologies (MWENT)* (pp. 1-5). IEEE.
[30] Tian, Meng., Y., X., Gu., Ran, Yang., Jing, Zong., Yihuai, Yang. (2023). Enhancing Communication Security with 3DES and Spread Spectrum Technologies. 2589 doi: 10.1088/1742-6596/2589/1/012016