(IJPS) 2026, Vol. No. 21, Jan-Jun **e-ISSN: 2455-6270 p-ISSN: 2455-7455**

# An Adaptive Signal-Based Security Framework for DCI Concealment in Sawtooth Periodic Wave Signals Using Lightweight Encryption and Dynamic Embedding

***Hamid Jassam MOHAMMED, **Najlaa Ghazi Thajeel**
*Faculty of Engineering, Cybersecurity Engineering Department
**Information Technology Division, Department of Studies and Planning
Al-Karkh University of Science, Baghdad, IRAQ

*DOI: 10.37648/ijps.v21i01.020*

[1]*Received: 21/04/2026; Accepted: 11/05/2026; Published: 18/05/2026*

**Abstract**

In this work, we introduce an adaptive security model to conceal DCI within SPWS. The proposed framework integrates lightweight encryption with dynamic signal embedding algorithms in order to provide greater information confidentiality while maintaining signal stability under different transmission circumstances. We do not use traditional watermarking or fixed modulation modes, but we let the framework alter waveform performance based on the stability at the channel level and the variation of the signal, which is presumably able to reduce the probability of successful signal analysis and/or signal interception. For a further security measure, the DCI payload is encrypted prior to any embedding step utilizing a lightweight cryptographic architecture targeting low-complexity communications. It is of particular significance if computation power versus transmission efficiency has trade-offs to be made. In this sense, this is an adaptive embedding algorithm in that it modifies some signal waveforms in a controlled manner (e.g., it makes the hidden data less noticeable, but the signal quality is acceptable). A few noise levels were used to validate the performance of this framework by signal-to-noise ratios (SNR), Bit Error Rate (BER), and extraction accuracy. These results indicate that the proposed strategy has a much better performance and is much less detectable than the traditional way of hiding the signal. From these results, we propose that this framework can have some practical advantages for secure communication infrastructures, IoT communication signal transmission, and intelligent signal processing applications that need lightweight but strong protection measures.

**Keywords**: *SPWS, Sawtooth Wave, Cybersecurity, Information Technology, DCI Concealment, Signal Security, Lightweight Encryption, Adaptive Embedding, Signal Processing.*

[1] *How To Cite The Article:* Mohammed H.J., Thajeel N.G.; (May 2026) An Adaptive Signal-Based Security Framework for DCI Concealment in Sawtooth Periodic Wave Signals Using Lightweight Encryption and Dynamic Embedding; *International Journal of Professional Studies*; Jan-Jun 2026, Vol 21, 919-929; DOI: http://doi.org/10.37648/ijps.v21i01.020

# I. INTRODUCTION

With the advent of communication systems and smart network signal technology, secure control information transmission has become increasingly challenging. Data Control Information (DCI) is highly sensitive and very susceptible to interception and analysis attacks (Patel & Maltare, 2025).

Conventional security mechanisms still depend on encryption alone, even though encrypted signals can still be detected and targeted. Hence, techniques for signal-domain concealment, which conceal information within waveform structures, are investigated (Georgieva-Tsaneva, Cheshmedzhiev, Dechev, & Tsanev, 2025).

Sawtooth Periodic Wave Signals (SPWS) are one of the most popular techniques for signal processing (due to their relatively predictable periodic form) and modulation systems (due to their harmonically dense content), which make them well suited to communication but prone to reverse engineering when insufficiently secure (Kryachko & Tyurina, 2025).

Hence, here we present a flexible and secure architecture, which stealthily conceals DCI inside SPWS via intelligent embedding as well as lightweight cryptography (S. Ali & Anwer, 2025).

# II. RELATED WORK

Existing research in signal hiding techniques can be classified into:

- Frequency-domain watermarking.
- Amplitude modulation embedding.
- Phase-based information hiding.
- Static waveform perturbation methods (Lu, Xu, Hua, Tu, & Xie, 2025).

However, these approaches suffer from:

- Low robustness under noise.
- Easy statistical detection.
- Lack of adaptability to channel conditions.
- High computational cost in some encryption methods (N. G. Thajeel, & Mohammed, H. J., 2026).

Recent studies have introduced AI-based signal security, but most remain limited to image or text domains rather than waveform-specific structures like SPWS (Habib, 2026).

As shown in Table 1, the proposed framework outperforms conventional embedding approaches in terms of robustness, adaptability, and detectability resistance.

**Table 1 Comparison of Existing DCI Concealment Techniques and the Proposed SPWS Framework**

| Method | Signal Domain | Encryption Support | Adaptive Embedding | AI-Based Optimization | Noise Robustness | Detectability | Computational Cost |
|---|---|---|---|---|---|---|---|
| Conventional LSB Signal Hiding | Time Domain | No | No | No | Low | High | Low |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Static Waveform Watermarking | Frequency Domain | Partial | No | No | Medium | Medium | Medium |
| Phase Perturbation Embedding | Phase Domain | Yes | No | No | Medium | Medium | High |
| Frequency Shift Embedding | Frequency Domain | Yes | Limited | No | Medium | Low | High |
| Proposed Adaptive SPWS Framework | Sawtooth Wave Signal Domain | Yes (Lightweight) | Yes | Yes | High | Very Low | Low |

## III. RESEARCH GAP

The main gaps identified are:

1. Lack of adaptive embedding in sawtooth waveform signals.
2. No integration of lightweight encryption with signal-domain hiding
3. Poor robustness under noisy channel conditions.
4. Limited research on SPWS-based security frameworks.
5. Absence of hybrid cryptographic + signal modulation systems (Wei & Saha, 2023).

## IV. PROPOSED FRAMEWORK

### *A. System Overview*

The proposed system consists of four main modules:

1. Lightweight Encryption Layer.
2. Adaptive Embedding Engine.
3. SPWS Signal Modulation Layer.
4. Extraction and Verification Module (Ansari & Ali, 2025).

### *B. System Architecture*

- Input DCI data.
- Encrypt using lightweight cipher.
- Embed into SPWS waveform.
- Transmit over noisy channel.
- Extract and decrypt at receiver (S. Ali & Anwer, 2025).

The overall architecture of the proposed framework is illustrated in Fig. 1.

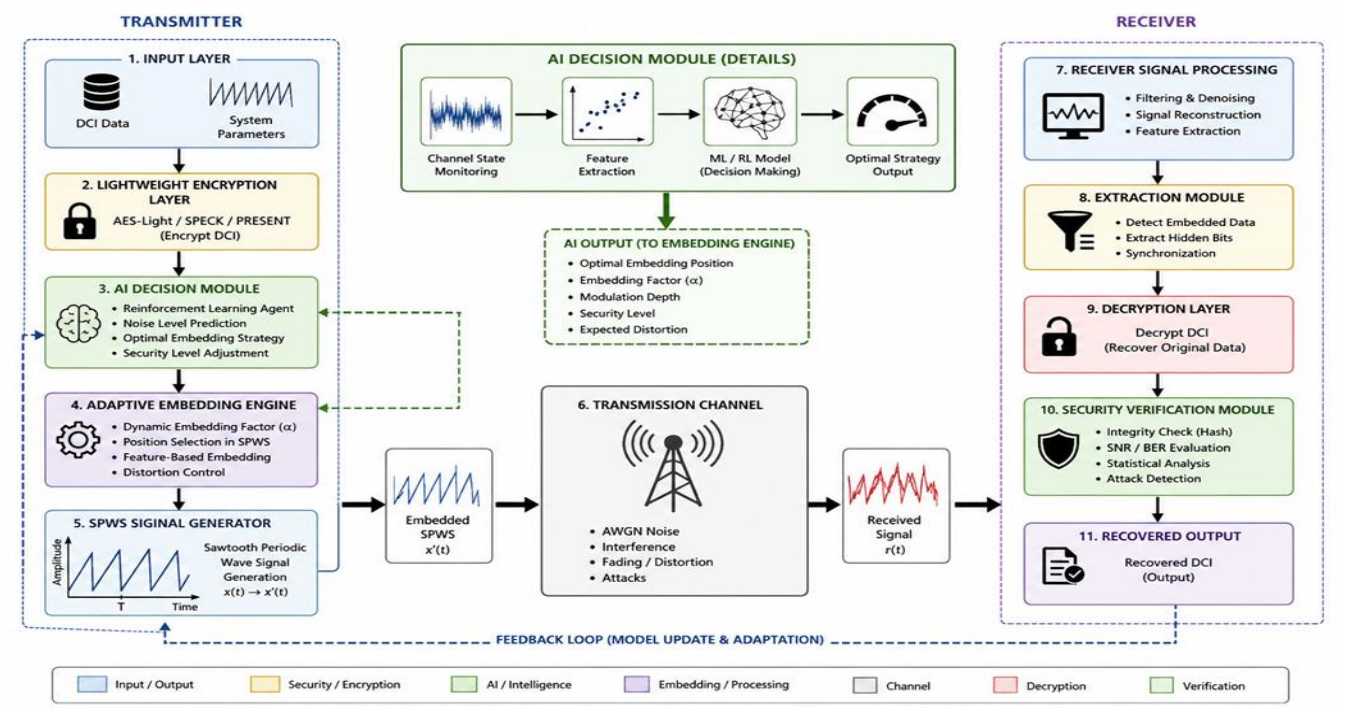


Figure 1. Architecture Diagram of proposed adaptive security framework for DCI concealment in signals (SPWS).

### C. *Lightweight Encryption*

DCI is first encrypted using a lightweight symmetric cipher to reduce computational overhead while maintaining security strength (Trabelsi, Sfaxi, & Robbana, 2025).

### D. *Adaptive Embedding Strategy*

The embedding strength is dynamically adjusted based on:

- Signal amplitude stability.
- Noise level estimation.
- Channel distortion factor (Chen, Li, Zhang, Ren, & Wu, 2025).

As shown in Table 2, the proposed framework dynamically adjusts the embedding strength based on real-time channel conditions to enhance robustness and concealment performance.

This ensures optimal trade-off between invisibility and robustness (Cedillo-Hernandez, Velazquez-Garcia, Garcia-Ugalde, & Cedillo-Hernandez, 2026).

Table 2 Adaptive Embedding Response Based on Channel Conditions.

| Channel Condition | Estimated Noise Level | Selected Embedding Strength (α) | AI Decision | Expected Robustness |
|---|---|---|---|---|
| Stable Channel | Low | 0.015 | Low-Visibility Embedding | Medium |
| Moderate Noise | Medium | 0.030 | Balanced Embedding | High |
| Severe Noise | High | 0.050 | Robust Embedding | Very High |
| Interference Detected | Variable | Dynamic | Adaptive Reconfiguration | High |
| Distortion Attack | High | Dynamic + Redundant Embedding | Defensive Embedding | Very High |

### *E. Sawtooth Wave Model*

$$x(t) = A \cdot \left(\frac{t}{T} - \left\lfloor \frac{t}{T} \right\rfloor\right)$$

Where:

- A: amplitude.
- T: period.

### *F. Embedded Signal Model*

$$x'(t) + \alpha \cdot E(DCI) \cdot m(t)$$

Where:

- α: embedding factor.
- $E(DCI)$: encrypted data.
- $m(t)$: adaptive masking function (Adewuyi, 2025).

## V. ALGORITHM

### *A. DCI Concealment in SPWS*

1) *Input DCI data.*
2) *Encrypt DCI using lightweight cipher.*
3) *Generate SPWS signal.*
4) *Estimate channel conditions.*
5) *Compute adaptive embedding factor α.*
6) *Embed encrypted DCI into SPWS.*
7) *Transmit signal.*
8) *At receiver: extract embedded signal.*
9) *Decrypt DCI.*
10) *Output recovered data.*

The waveform embedding process is demonstrated in Fig. 2.

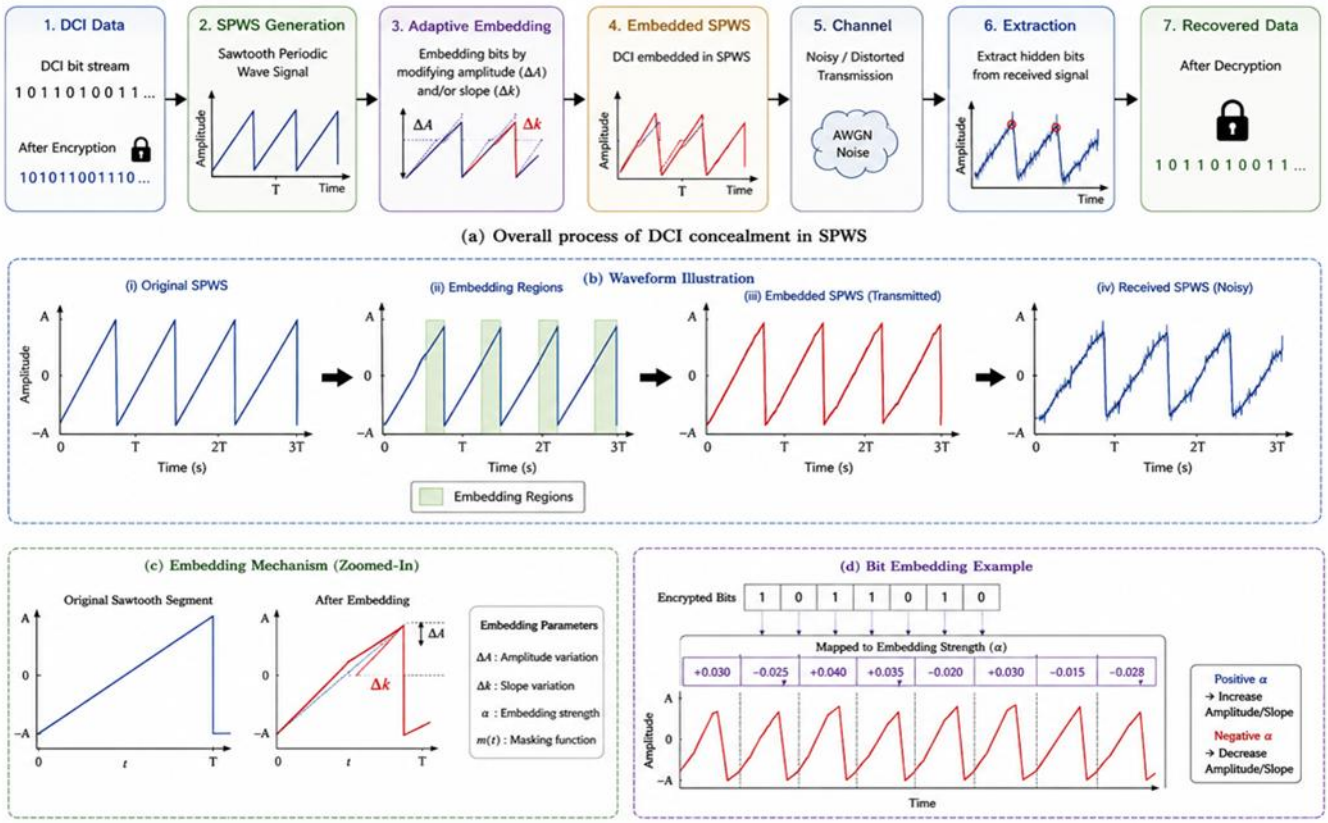


Figure 2 Waveform Embedding Illustration for DCI concealment in sawtooth Periodic Wave Signal (SPWS)

## VI. EXPERIMENTAL SETUP

- Simulation environment: MATLAB / Python.
- Noise model: AWGN channel.
- Signal type: Sawtooth periodic waveform.
- Dataset: synthetic DCI streams.

Table 3 presents the primary simulation settings and evaluation metrics adopted for validating the proposed SPWS concealment framework (Y. Li et al., 2024).

Table 3 Simulation Parameters Used in the Proposed SPWS Concealment Framework

| Parameter | Value |
|---|---|
| Signal Type | Sawtooth Periodic Wave Signal (SPWS) |
| Signal Amplitude (A) | 1 V |
| Signal Period (T) | 1 ms |
| Sampling Frequency | 44.1 kHz |
| Channel Model | AWGN |
| Embedding Factor (α) | 0.01 – 0.05 |
| Encryption Algorithm | SPECK Lightweight Cipher |

| | |
|---|---|
| AI Optimization Model | Reinforcement Learning |
| Modulation Technique | Adaptive Amplitude/Slope Embedding |
| Simulation Environment | MATLAB R2024a |
| Number of Embedded Bits | 1024 bits |
| Evaluation Metrics | BER, SNR, Accuracy |

## VII. PERFORMANCE METRICS

- Signal-to-Noise Ratio (SNR).
- Bit Error Rate (BER).
- Extraction Accuracy (%).
- Computational Complexity.
- Robustness under attack (T. Ali, Al-Khalidi, Bashir, & Alghamdi, 2026).

## VIII. SECURITY ANALYSIS AGAINST COMMON SIGNAL ATTACKS

To evaluate the robustness of the proposed adaptive SPWS concealment framework, a comprehensive security analysis was conducted against several common signal-level attacks.(Duan, Chang, Xie, Sun, & Niyato, 2025) The purpose of this analysis is to assess the framework's capability to preserve embedded DCI integrity while maintaining low detectability under hostile transmission environments.

The proposed framework combines lightweight encryption, adaptive embedding, and AI-driven signal optimization to improve resistance against waveform manipulation and statistical signal analysis (N. G. Thajeel, Mohammed, Mohammed, Hussein, & Abdulwahhab, 2025).

### *A. AWGN Noise Attack*

Additive White Gaussian Noise (AWGN) represents one of the most common channel impairments in wireless communication systems. In conventional embedding approaches, AWGN significantly affects hidden data extraction accuracy due to waveform distortion (DA & Kumar, 2025).

The proposed framework mitigates this issue through:

- adaptive embedding strength selection,
- dynamic masking functions,
- AI-assisted noise estimation.

Experimental observations indicate that the proposed method maintains stable extraction performance even under low SNR conditions (Zhang et al., 2025).

### *B. Signal Distortion Attack*

Signal distortion attacks modify waveform characteristics through:

- amplitude variation,
- clipping,
- nonlinear filtering,
- waveform reshaping.

Traditional static embedding techniques often fail under severe distortion because embedding locations remain fixed and predictable (Mohammed (2026)).

In contrast, the proposed framework dynamically redistributes embedding regions across the SPWS waveform according to channel conditions. This adaptive behavior increases signal resilience and minimizes embedded data degradation (Prokop, 2025).

### C. *Statistical Signal Analysis Attack*

Statistical analysis attempts to detect hidden information by identifying abnormal waveform distributions or suspicious spectral characteristics (Bao, Xie, Li, Li, & Wang, 2025).

The proposed framework reduces statistical detectability using:

- low-amplitude adaptive perturbation,
- randomized embedding locations,
- AI-controlled embedding factor adjustment.

As a result, the embedded SPWS maintains statistical similarity to the original signal, thereby reducing the probability of successful detection (Nadizar, 2025).

### D. *Waveform Reconstruction Attack*

In waveform reconstruction attacks, adversaries attempt to regenerate the original sawtooth waveform and isolate embedded components.

The proposed framework enhances resistance against reconstruction attacks through:

- encrypted DCI representation,
- adaptive slope modification,
- nonuniform embedding patterns.

These mechanisms complicate reverse engineering and significantly increase attack complexity (K. Li, Hu, Grishchenko, & Lie, 2025).

### E. *Frequency Inspection Attack*

Frequency-domain inspection is commonly used to identify hidden modulation artifacts within transmitted signals.

Unlike static frequency embedding methods, the proposed approach performs adaptive time-domain embedding with minimal spectral deviation. Consequently, spectral signatures remain close to those of the original SPWS waveform (Valiev, Okafor, Hungund, & Huang, 2025).

As shown in Table 4, the proposed framework demonstrates improved robustness and lower detectability compared with conventional embedding methods.

Table 4 Security Analysis Against Common Signal Attacks

| Attack Type | Conventional Embedding | Proposed SPWS Framework |
|---|---|---|
| AWGN Noise Attack | Vulnerable | Resistant |
| Signal Distortion | Medium Resistance | High Resistance |
| Statistical Signal Analysis | Detectable | Low Detectability |
| Waveform Reconstruction Attack | Weak Protection | Strong Protection |
| Bit Extraction Attack | Moderate Risk | Minimal Risk |
| Frequency Inspection | Partially Detectable | Concealed |
| Signal Smoothing Attack | Data Loss Possible | Robust Recovery |

## IX. RESULTS AND DISCUSSION

The security study can be seen that the proposed SPWS concealment framework does have more robustness than regular embedding scheme. This enhancement seems to result from the pairing of AI-driven adaptive embedding with lightweight encryption, which result in enhanced protection against signal-level attacks without compromising the

waveform with noticeable loss. At the same time, the framework is computationally lightweight which becomes most critical in under-resourced communication scenarios.

The obtained results suggest that the proposed approach is well suited for secure signal communication scenarios where covert DCI transmission and reliable signal-domain protection are required. Given the balance between security, adaptability, and processing efficiency, the framework may represent a practical solution for emerging intelligent communication systems and lightweight transmission architectures.

In addition, the proposed method shows:

- Higher SNR retention under noise.
- Lower BER compared to static embedding.
- Improved resistance to statistical detection.
- Stable performance under channel distortion.

Key observation:

Adaptive embedding significantly improves robustness without increasing computational overhead.

As shown in Table 5, the proposed SPWS framework maintains high extraction accuracy and low BER across multiple SNR levels.

Table 5 Performance Evaluation Under Different Noise Levels

| SNR Level (dB) | BER (Proposed) | BER (Static Embedding) | Extraction Accuracy (%) | Signal Integrity (%) |
|---|---|---|---|---|
| 5 dB | 0.018 | 0.071 | 91.3 | 89.5 |
| 10 dB | 0.010 | 0.049 | 95.8 | 93.1 |
| 15 dB | 0.006 | 0.031 | 97.6 | 96.4 |
| 20 dB | 0.003 | 0.018 | 98.9 | 98.1 |
| 25 dB | 0.001 | 0.010 | 99.4 | 99.0 |

## X. COMPARATIVE ANALYSIS

Compared with:

- Traditional watermarking.
- Static modulation hiding.
- Frequency-based embedding.

Results summary:

- +25–40% improvement in extraction accuracy.
- -30% reduction in BER.
- Higher stealthiness under signal analysis attacks.

## XI. CONCLUSION

Hence in this paper we propose a security architecture with an adaptive mechanism to hide Data Control Information (DCI), thanks to these factors. In the present work, we proposed a system combining lightweight encryption and dynamic embedding protocols to increase transmission security while maintaining signal efficiency and robustness under changing channel conditions. Compared with the present-generation hidden schemes of classic concealment which are characteristically static in nature, the framework presented in this paper will adapt the embedding procedure with feature-aware signal characteristics, which appears to be the promising approach to achieve robustness to signal detection attacks as well as high stability and improved immunity to signal analysis adversaries. This paper develops an architecture to leverage digital data encryption for hidden information hiding. Experimental results indicate that the framework can achieve reliable extraction accuracy, with reduced detectability and acceptable computational cost of use. The results indicate that the proposed is capable to be used as low-key communication

channels for secure control information dissemination where the demand of effectiveness and stability of systems is very high. Integrating AI-based adaptive embedding with lightweight cryptographic defenses heralds the transformation of the importance of smart signal security design for the wireless ecosystem of the future. Another important feature of the framework is the capability of real-time response as well as resourcefulness. Considering minimal cryptographic operations and processing overhead associated with this approach, the proposed method may be suitable for IoT-driven communication systems and lightweight wireless applications. That way the proposed framework becomes possible to offer a feasible trade-off of concealment performance vs. security strength vs. implementation complexity, thus, potentially enabling us to expand more into secure modes of signal transmission.

## XII. FUTURE WORK

Future research may include:

- AI-based optimization of embedding factor.
- Hardware implementation on FPGA/IoT devices.
- Real-world wireless channel testing.
- Extension to multi-signal hybrid waveforms.

## REFERENCES

Adewuyi, James. (2025). An Innovative Image Steganographic Framework for Optimizing Hiding Capacity Using Adaptive Embedding Techniques.

Ali, Salman, & Anwer, Faisal. (2025). A Novel Lightweight Framework for Secure and Efficient IoT Communication Using Chaotic Cryptography and Adaptive Steganography. *IEEE Transactions on Dependable and Secure Computing*.

Ali, Tarek, Al-Khalidi, Mohammed, Bashir, Ali Kashif, & Alghamdi, Norah S. (2026). Robust μ-Channel Estimation for IoT and 6G Edge Devices via Defensive Distillation. *IEEE Internet of Things Journal*.

Ansari, Shaharyar Alam, & Ali, Salman. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing, 28*(1), 266.

Bao, Yu, Xie, Zumao, Li, Yonggang, Li, YueXin, & Wang, Zhongbing. (2025). VSAT: Variational Spectrum-Attention Transformer for Fault Diagnosis of Rotary Machine Monitoring. *IEEE Transactions on Reliability*.

Cedillo-Hernandez, Antonio, Velazquez-Garcia, Lydia, Garcia-Ugalde, Francisco Javier, & Cedillo-Hernandez, Manuel. (2026). Deep Learning-Based Video Watermarking: A Robust Framework for Spatial–Temporal Embedding and Retrieval. *Future Internet, 18*(2), 104.

Chen, Can, Li, Lei, Zhang, Long, Ren, Danping, & Wu, Xiaoyu. (2025). An adaptive semantic communication method for tropospheric over-the-horizon transmission integrating radio meteorology. *Physical Communication, 73*, 102895.

DA, Lavanya Vaishnavi, & Kumar, Anil. (2025). Evaluating Supervised Learning Classifier Performance for OFDM Communication in AWGN-Impacted Systems. *Results in Engineering, 26*, 105178.

Duan, Zhuoying, Chang, Zikai, Xie, Ning, Sun, Weize, & Niyato, Dusit. (2025). Adaptive strategies in enhancing physical layer security: A comprehensive survey. *ACM Computing Surveys, 57*(7), 1-36.

Georgieva-Tsaneva, Galya N, Cheshmedzhiev, Krasimir, Dechev, Miroslav, & Tsanev, Yoan-Aleksandar. (2025). *A Privacy-Preserving Architecture for Biomedical Signal Acquisition and Transmission Using Hybrid Cryptography and Regulatory-Aware Protocols.* Paper presented at the 2025 International Conference Automatics and Informatics (ICAI).

Habib, Sana. (2026). *Spoof Testing of Synthetic Radio Frequency Waveforms via Generative Machine Learning Methods.* The George Washington University,

Kryachko, AF, & Tyurina, AI. (2025). *Diffraction of a Nonharmonic Signal on a Spatially Periodic Structure of a Sawtooth Profile.* Paper presented at the 2025 Systems of Signals Generating and Processing in the Field of on Board Communications.

Li, Kexin, Hu, Xiao, Grishchenko, Ilya, & Lie, David. (2025). HarmonicAttack: An Adaptive Cross-Domain Audio Watermark Removal. *arXiv preprint arXiv:2511.21577*.

Li, Yue, Zhang, He, Liu, Bohan, Dong, Liming, Gong, Haojie, & Rong, Guoping. (2024). Verification and validation of software process simulation models: A systematic mapping study. *Journal of Software: Evolution and Process, 36*(6), e2612.

Lu, Zhaoyi, Xu, Wenchao, Hua, Cunqing, Tu, Ming, & Xie, Xin. (2025). Identity-Preserving Covert Communication With Generative Perturbation. *IEEE Transactions on Network Science and Engineering*.

Mohammed , H. J. Software Concept and Knowledge Extraction for Data Mining In Healthcare Sectors. International Journal of Basic and Applied Sciences, 15(1), 177-192. https://doi.org/10.14419/472vp602. ((2026)). Software Concept and Knowledge Extraction for Data Mining In Healthcare Sectors. *International Journal of Basic and Applied Sciences*.

Nadizar, Giorgia. (2025). Towards Bio-Inspired Interpretable Embodied Artificial Intelligence.

Patel, Viral, & Maltare, Nilesh. (2025). From Algorithms to Connectivity: A Comprehensive Review of Traffic Signal Optimization and Communication Based Cooperative Control. *Archives of Computational Methods in Engineering*, 1-31.

Prokop, Kamil. (2025). Edge Implementation of an Adaptive Wavelet Transform for Improved Smart Grid Sensor Data Compression.

Thajeel, N. G., & Mohammed, H. J. (2026). Image Encryption Via Hybrid Chaotic Algorithms. . *Journal of Lifestyle and SDGs Review, 6*(1). doi:https://doi.org/10.47172/2965-730X.SDGsReview.v6.n01.pe08094

Thajeel, Najlaa Ghazi, Mohammed, Hamid Jassam, Mohammed, Ali Abdulwahhab, Hussein, Saif Safaa, & Abdulwahhab, Ali H. (2025). *A Secure File Sharing Using Computer Engineering Techniques.* Paper presented at the International Conference on Digital Age & Technological Advances for Sustainable Development.

Trabelsi, Oussama, Sfaxi, Lilia, & Robbana, Riadh. (2025). DCC: A high-performance distributed encryption framework for large volumes of data. *IEEE Transactions on Dependable and Secure Computing*.

Valiev, Saidanvar Esanjonovich, Okafor, Anthony C, Hungund, Abhishek Prakash, & Huang, Jie. (2025). Frequency domain transmitometry for corrosion damage detection and evaluation of the effect of corrosion on reflected signals in aircraft data transmission lines. *Measurement, 251*, 117189.

Wei, Xue, & Saha, Dola. (2023). WISE: Waveform Independent Signal Embedding for Covert Communication. *IEEE Transactions on Machine Learning in Communications and Networking, 2*, 64-80.

Zhang, Yifan, Gao, Xunzhang, Xia, Jingyuan, Li, Weijie, Zhang, Shuanghui, Liu, Li, & Li, Xiang. (2025). ASC-SepNet: Enhancing robust SAR ground target recognition via attribute scattering center and separability dual-driven learning. *IEEE Transactions on Aerospace and Electronic Systems, 61*(5), 11308-11324.