Journal of Computational and Applied Mathematics 474 (2026) 116932

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Masking of measurements in a photovoltaic system using an incommensurate fractional-order chaotic system based on string dynamics around the Bardeen-AdS black hole

Haris Calgan [a,*], Abdullah Gokyildirim [b], Suleiman M. Sharkh [c], Metin Demirtas [a]

[a] Department of Electrical and Electronics Engineering, Faculty of Engineering, Balikesir University, Cagis Campus, Balikesir, 10145, Turkiye
[b] Department of Electrical and Electronics Engineering, Faculty of Engineering, Bandirma Onyedi Eylul University, Bandirma, Balikesir, 10200, Turkiye
[c] Mechatronics Research Group, Faculty of Engineering and Physical Sciences, University of Southampton, Southampton, SO171BJ, United Kingdom

ARTICLE INFO

Keywords:
Chaos
PV system
Fractional-order
Cosmology
Cybersecurity
Encryption

ABSTRACT

Considering environmental factors and global warming, the use and installation of photovoltaic (PV) systems have become widespread. However, the integration of these PV systems into smart grids raises concerns regarding cybersecurity. Since PV systems rely on communication networks, remote monitoring, and grid-connected inverters, they exhibit a cyber–physical structure and are therefore vulnerable to cyber-attacks. Cyber threats targeting PV infrastructure can lead to system failures, energy theft, grid instability, and financial losses. While many studies focus on cyber-attack detection for PV system cybersecurity, this paper aims to design a cybersecure PV system by employing a novel chaos-based encryption method. Due to their unpredictable and highly sensitive nature, chaotic algorithms are utilized to ensure secure communication within PV systems. The encryption algorithm is derived from the incommensurate fractional analysis of the "strings around the Bardeen-AdS black hole surrounded by quintessence dark energy", a cosmological system. Simulation results performed in MATLAB/Simulink confirm the effectiveness of the proposed encryption framework. The underlying pseudo-random number generator (PRNG) successfully passed all 15 standard NIST SP800-22 statistical tests, validating its strong statistical randomness and unpredictability. Furthermore, the encrypted signals consistently exhibit high information entropy (e.g., V_{PV} encrypted entropy = 5.3213 compared to actual entropy = 4.0931), indicating strong randomization and obscurity of original patterns. The decrypted outputs precisely recover the original measurements, with entropy values perfectly matching the actual signals (e.g., decrypted V_{PV} entropy = 4.0931), thereby validating the reliability, reversibility, and cyber resilience of the approach.

1. Introduction

The increased utilization of renewable energy sources has become a global objective due to environmental concerns and the urgent need to reduce greenhouse gas emissions. Among various renewable energy technologies, PV systems have gained prominence not only because they directly convert solar energy into electricity, but also due to their lower cost compared to traditional fossil

* Corresponding author.
E-mail addresses: haris.calgan@balikesir.edu.tr (H. Calgan), agokyildirim@bandirma.edu.tr (A. Gokyildirim), S.M.Sharkh@soton.ac.uk (S.M. Sharkh), mdtas@balikesir.edu.tr (M. Demirtas).

https://doi.org/10.1016/j.cam.2025.116932
Received 28 April 2025; Received in revised form 8 July 2025
Available online 8 August 2025

fuel-based power generation [1]. However, the growing adoption of PV systems and their integration into smart grids introduce new challenges, particularly in the domain of cybersecurity [2]. Since PV systems rely on digital communication networks, they are susceptible to various cyber-attacks that can compromise their security and functionality.

Cybersecurity risks in PV systems arise from their cyber–physical nature, making them potential targets for malicious activities such as unauthorized access, data manipulation, and denial-of-service (DoS) attacks. A successful cyber-attack on PV infrastructure can lead to energy theft [3], operational disruptions [4], voltage instabilities [5], and even large-scale cascading failures [6]. As cyber-attacks targeting critical energy infrastructure continue to rise [7,8], ensuring the security of PV systems has become essential for maintaining the stability and reliability of modern energy networks.

Numerous studies have been conducted in the literature to address cybersecurity concerns in PV systems. A comprehensive review of the current literature reveals a diverse set of strategies aimed at securing PV infrastructures. Zhang et al. (2020) emphasize that smart PV systems, particularly those integrated with Maximum Power Point Tracking (MPPT) and IoT-based monitoring, are increasingly susceptible to cyber threats due to their distributed and interconnected architectures [9]. Arbab-Zavar et al. (2022) address the impact of communication link failures on PV included microgrid control and management, proposing deep learning-based generation and consumption forecasting to mitigate these effects [2]. As PV farms incorporate more power electronics and digital control mechanisms, their vulnerability to sophisticated cyber-attacks proportionally increases. To address this, emerging solutions such as waveform-based detection techniques have been introduced to accurately distinguish between physical faults and cyber intrusions in real time [5]. In particular, data integrity attacks targeting DC–DC and DC–AC converters have drawn significant attention, leading to the growing adoption of deep learning models for real-time threat detection in PV-based smart grid environments [10]. Kim et al. (2024) propose a dynamic watermarking-based architecture designed to enhance the cybersecurity of solar PV power distribution networks [11]. Similarly, Dayarathne et al. (2025) introduce a hybrid security model that combines deep learning techniques with conventional anomaly detection methods to defend against complex threats within Cyber–Physical Power Systems (CPPS) [12].

Blockchain-based security solutions have also been explored. Subramaniam et al. (2025) present a blockchain-enhanced framework to improve the immutability and auditability of data transactions within smart DC microgrids incorporating PV systems [13]. Additionally, Tufail et al. (2025) develop a hybrid machine learning framework that integrates Principal Component Analysis (PCA) with stacked autoencoders to detect false data injection attacks in PV-based smart grids [14]. The increasing reliance on renewable energy sources, particularly solar and wind, and the concurrent rise in cyber threats underscore the dual challenges faced by smart grid infrastructures. Biswas et al. (2025) emphasize the necessity of robust, adaptive strategies to address these twin challenges effectively [15].

The integration of Hybrid Renewable Energy Systems (HRES) with smart grid Information and Communication Technology (ICT) infrastructures further amplifies the need for advanced cybersecurity measures. A recent study introduces a deep learning-based security framework that incorporates fuzzy logic and a robust key management scheme to enhance data routing and system protection [16]. In a complementary vein, Harrou et al. (2023) provide a detailed overview of the key cybersecurity threats and vulnerabilities unique to PV systems, offering a foundational understanding for developing future mitigation strategies [17].

A summary of the literature reveals that existing cybersecurity measures commonly include encryption techniques, intrusion detection systems (IDS), and firewalls. However, as cyber-attacks become more sophisticated, these conventional defenses often fall short in ensuring end-to-end data protection. In this context, chaotic systems offer a promising alternative due to their deterministic yet unpredictable behavior, which is ideal for encryption, key generation, and secure communication protocols [18,19]. Therefore, chaotic systems, due to their extreme sensitivity to initial conditions and inherent unpredictability, are highly effective for secure encryption, authentication, and data transmission [20,21]. In this regards, chaos-based cryptography has garnered increasing attention in recent years, particularly in domains like wireless sensor networks, industrial control systems, and smart grids [22–24]. The use of chaos theory in secure systems leverages properties such as ergodicity, and topological mixing, all of which are highly desirable in cryptographic applications [25,26].

More recently, fractional-order chaotic systems have been explored as a powerful tool to design more secure and flexible encryption frameworks, since the additional fractional-order parameters introduce richer dynamics and extended key spaces [27]. In particular, incommensurate fractional-order (IFO) models have demonstrated improved resistance against classical attacks such as brute-force, statistical, and differential attacks due to their high complexity [28]. Furthermore, chaotic sequences derived from physical systems, such as those described by relativistic mechanics or general relativity, introduce a novel intersection between physics and cybersecurity [29,30]. This interdisciplinary approach not only strengthens security but also opens new research avenues that bridge nonlinear dynamics, information theory, and renewable energy systems.

Despite these promising developments, a limited number of studies have applied chaos-based cryptography specifically to PV systems. This study proposes a novel approach to securing PV systems using a chaos-based encryption method inspired by theoretical physics. Specifically, the encryption algorithm is developed based on the incommensurate fractional analysis of the strings around the Bardeen-AdS black hole surrounded by quintessence dark energy [30]. This unique methodology leverages advanced mathematical models to generate cryptographic sequences, thereby enhancing the security of PV communications. By implementing this encryption technique, the protection of PV systems can be significantly improved, ensuring the safe operation of renewable energy infrastructures. To evaluate the effectiveness of the proposed method, simulation studies have been conducted on a PV system modeled in Matlab/Simulink. This research highlights the potential of chaos-based methodologies in strengthening the resilience of smart grid-connected PV systems, offering a new perspective on cybersecurity strategies for future energy networks.

The rest of the paper is organized as follows: Section 2 introduces the concept of strings around the Bardeen–AdS black hole in the presence of quintessence dark energy, along with IFO analysis, numerical simulations, and bifurcation diagrams. Section 3

presents the design and implementation of a lightweight encryption scheme for a grid-connected PV system based on a fractional-order chaotic system. This includes system architecture, PRNG design, data encryption/decryption stages, and numerical validation. Section 4 evaluates the encryption algorithm's performance through key space, histogram, and entropy analyses. Finally, Section 5 concludes the paper and suggests future research directions.

2. Incommensurate fractional-order analysis of strings around the Bardeen-AdS black hole surrounded by quintessence dark energy

In this section, an IFO analysis is conducted to investigate the behavior of strings around a Bardeen-AdS black hole surrounded by quintessence dark energy. A concise theoretical background is first provided, followed by a numerical analyses. Finally, the system's dynamical characteristics are examined through bifurcation diagrams and spectral entropy measurements.

2.1. Brief definition

The Bardeen-AdS black hole represents a non-singular solution to Einstein's equations, made possible by the inclusion of a nonlinear electromagnetic field [31]. This feature ensures the black hole remains free of singularities, meaning it behaves regularly throughout spacetime. The black hole exists within a four-dimensional anti-de Sitter (AdS) spacetime, influenced by a negative cosmological constant, which helps shape the geometry of this spacetime [32].

Surrounding the black hole is quintessence, a proposed form of dark energy, which introduces additional complexity into the system. Quintessence is characterized by parameters such as the state parameter ω_q and energy density ρ_q, both of which play crucial roles in altering the behavior of the spacetime structure, including the formation of event horizons. The metric function of the black hole is derived by considering the effects of quintessence, showing how changes in ω_q can lead to different physical outcomes [33].

The motion of the string is described using the Polyakov action, which takes into account the target space coordinates and the string's winding number. The equations of motion derived from the Lagrangian reveal the complex interplay between the string's motion and the surrounding spacetime geometry. Three potential modes of motion for the string are identified: oscillation around the black hole, eventual falling into the black hole, or escaping to infinity after several oscillations [34].

A recent study [30] has focused on how the quintessence parameters a (normalization constant) and ω_q influence the string's behavior. In particular, different values of these parameters lead to varying degrees of chaotic or regular motion. For instance, when $\omega_q = -1/3$, the string's motion becomes more chaotic, while $\omega_q = -2/3$ leads to more regular, ordered behavior. Numerical simulations of the system illustrate how the string's radius and angular components change over time, offering insights into the chaotic dynamics near the Bardeen-AdS black hole. Briefly, the following canonical equation defines the motion of one circular string in the context of Bardeen-AdS black holes [30]:

$$\begin{aligned}
\dot{r} &= \pi a' f P_r, \\
\dot{P}_r &= -\frac{\pi a'}{2} f' P_r^2 - \frac{\pi a' P_t^2 f'}{2 f^2} + \frac{\pi a' P_\theta^2}{r^3} - \frac{n^2 r \sin^2\theta}{\pi a'}, \\
\dot{\theta} &= \frac{\pi a' P_\theta}{r^2}, \\
\dot{P}_\theta &= -\frac{n^2 r^2 \sin\theta\cos\theta}{\pi a'}.
\end{aligned} \tag{1}$$

In Eq. (1), P_r, P_θ and P_t denote canonical momenta. String radius varies over time is defined as $R(\tau) = r\sin\theta$ where θ is string angle. $f(r)$ corresponds to the Bardeen-AdS black hole encircled by the quintessence as given in Eq. (2).

$$f(r) = 1 - \frac{2Mr^2}{(r^2+\beta^2)^{3/2}} + \frac{r^2}{l^2} - \frac{a}{r^{3\omega_q+1}} \tag{2}$$

The dot in the superscript signifies the derivative with respect to τ, and the superscript symbol '′' is used hereafter to stand for the derivative with respect to r. Hence $f'(r)$ can be calculated as in Eq. (3).

$$f'(r) = -\frac{2Mr(2r^2+3\beta^2)}{(r^2+\beta^2)^{5/2}} + \frac{2r}{l^2} + a(3\omega_q+1)r^{-(3\omega_q+2)} \tag{3}$$

The parameters given in between Eqs. (1) and (3) can be summarized as follows: l is the AdS radius, ω_q is the quintessence state parameter, a is positive normalization constant, M is black hole mass, β corresponds to magnetic monopole charge, a' relates the string length, n is winding number. To ensure the presence of chaotic dynamics essential for our encryption scheme, the parameters for system (1) were adopted from Ref. [30], where chaotic behavior has been previously identified using the following values: $a = 0.02$, $\beta = 0.02$, $M = 0.2$, $n = 1$, $a' = 1/\pi$, $l = 15$, $\omega_q = -1/3$, $P_t = 12$ while the initial conditions are as follows: $r(0) = 10$, $P_r(0) = 2.670855$, $\theta(0) = 0$. A seventh-eight order continuous Runge–Kutta method has been adopted to solve the equations of motion of one circular string. Fig. 1 illustrates the chaotic behavior of the integer-order system given in Eq. (1). However, fractional-order analysis of this system has not been conducted yet even if the system is commensurate or IFO. Therefore, in the subsequent subsection, we focus on performing the IFO analysis of system (1), providing new insights into its dynamics.

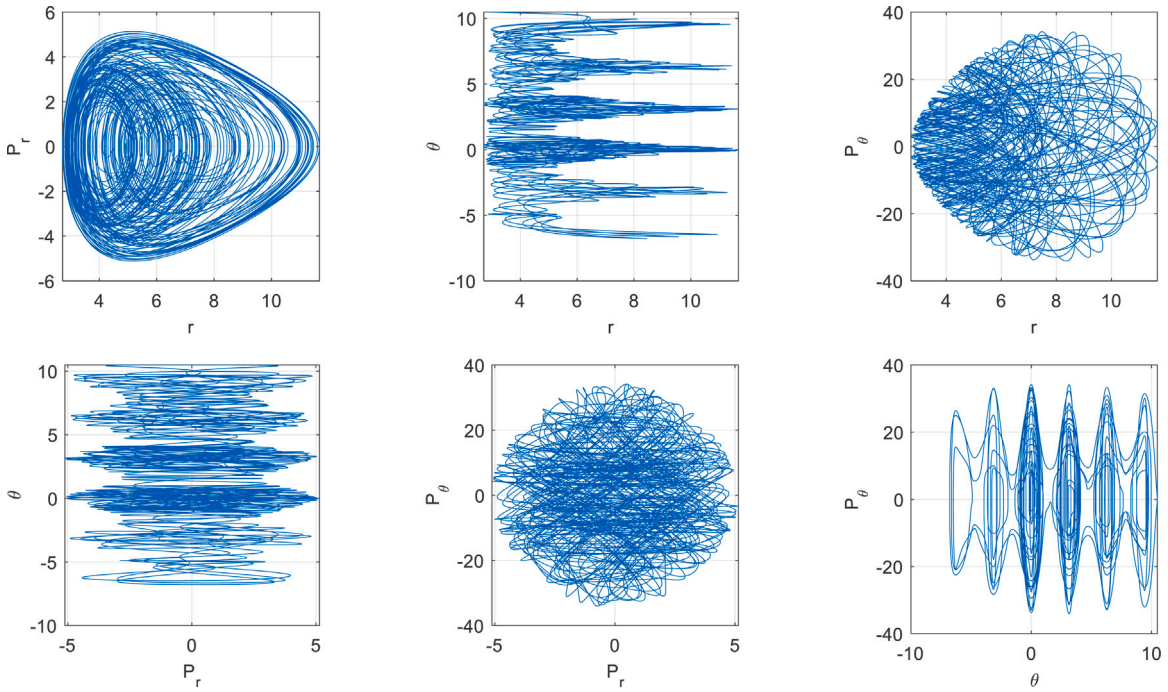

Fig. 1. Chaotic phase portraits of system integer-order system given in Eq. (1).

2.2. Numerical analyses

Based on the canonical equations of motion given in Eq. (1) and the Bardeen-AdS black hole metric function influenced by quintessence in Eq. (2) and its radial derivative in Eq. (3), the dynamical behavior of the system is investigated through phase portraits, bifurcation diagrams, and spectral entropy analysis. These tools are essential for analyzing the nonlinear characteristics of the circular string's motion under the influence of varying fractional derivatives and quintessence parameters. To numerically solve the resulting incommensurate fractional-order (IFO) differential equations, the well-established Adams–Bashforth–Moulton predictor–corrector method is employed using the MATLAB toolbox "fde12" developed by Garrappa [35,36]. This method is particularly suited for fractional differential equations formulated in the Caputo sense, which allows for physically meaningful initial conditions.

It is worth mentioning that several other fractional derivative definitions also exist in the literature. For example, the Riemann–Liouville (RL) definition, although mathematically elegant, poses limitations in practical applications since it requires initial conditions defined in terms of fractional integrals, which are often not physically intuitive. Similarly, the Grünwald–Letnikov (GL) derivative is known for its straightforward discretization and frequent use in numerical schemes, but it may suffer from instability and step-size sensitivity, especially in systems with chaotic or stiff behavior [37]. More recently, the Atangana–Baleanu (AB) derivative in the Caputo sense has gained attention for incorporating a non-singular and non-local Mittag–Leffler kernel, which provides a more realistic representation of memory effects in physical processes [38,39]. However, its numerical implementation remains computationally more demanding and lacks the solver maturity of Caputo-based approaches. Given these considerations, the Caputo derivative was selected in this work as it offers a good balance between mathematical tractability, physical interpretability, and availability of reliable numerical solvers.

Bifurcation diagram analysis was conducted to quantitatively demonstrate chaotic behaviors as the parameter a is varied. As illustrated in Fig. 2a, the bifurcation diagram of the integer-order system reveals complex dynamic transitions. For a values approximately between -0.75 and -0.25, the system exhibits periodic behavior, characterized by distinct, well-defined branches of max(Y) values. As a increases beyond this range, specifically around $a = -0.25$, the system undergoes period-doubling bifurcations, leading to an increase in the number of possible states for max(Y). This period-doubling cascade continues, and for $a > 0$, the system clearly transitions into chaotic dynamics, indicated by the wide scattering of max(Y) values, particularly evident as a approaches 0.8. The diagram distinctly shows that beyond the initial periodic windows, the system's behavior becomes highly unpredictable and sensitive to the parameter a, with max(Y) values spanning a broad range, reaching up to approximately 22–23 for a close to 0.8. These results confirm that the nonlinear response of the integer-order system (1) is highly sensitive to the choice of the normalization parameter a, showcasing a clear route to chaos through period-doubling.

Fig. 2b illustrates the bifurcation diagram for the commensurate fractional-order system, where the parameter q is varied and $a = 0.2$. For values of q less than approximately 0.985, the system exhibits stable, possibly fixed-point or very low-amplitude periodic

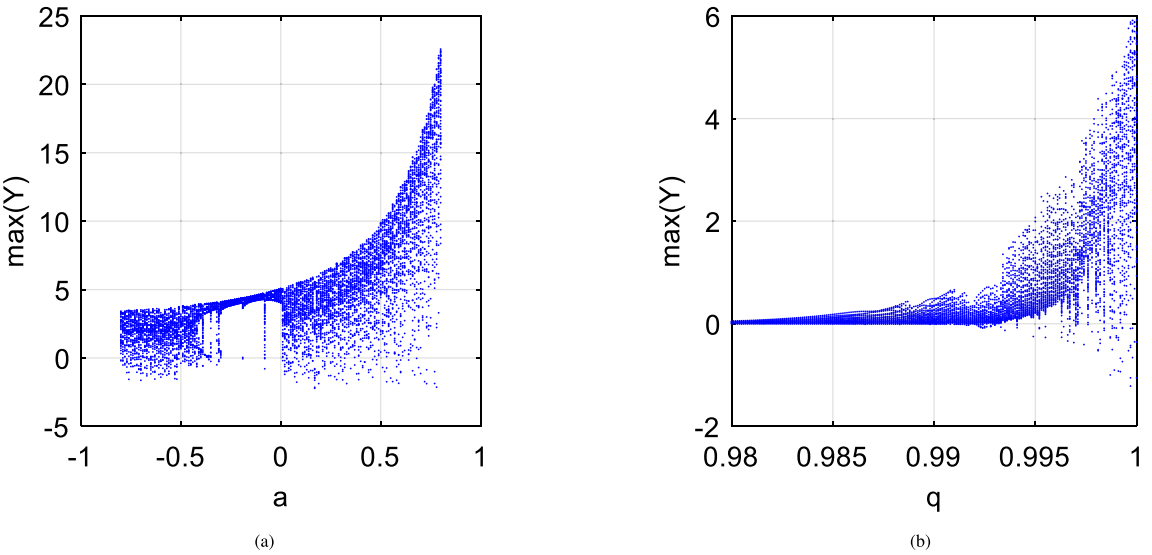

Fig. 2. Bifurcation diagrams (a) integer-order system (b) commensurate FO system.

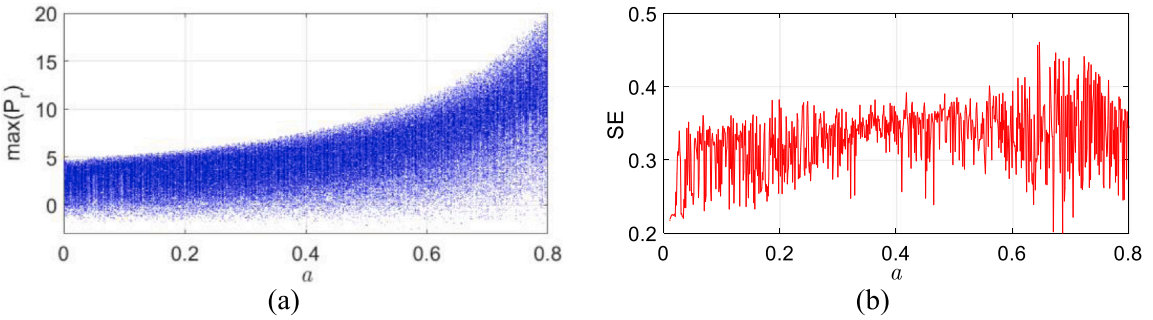

Fig. 3. Dynamic analyses of system (1) for bifurcation parameter a for $q_1 = 0.997$, $q_2 = 0.998$, $q_3 = 0.999$ and $q_4 = 1$: (a) bifurcation diagram (b) spectral entropy diagrams.

behavior, as indicated by the consistently low values of max(Y) centered around zero. As q increases from 0.985 towards 0.99, a subtle broadening of the max(Y) values suggests the onset of oscillatory or more complex periodic dynamics. Beyond $q \approx 0.99$, the system clearly transitions into chaotic behavior, characterized by a significant spread of max(Y) values. This chaotic region becomes increasingly pronounced as q approaches 1, with max(Y) values spanning a range from negative values to approximately 6. This diagram highlights the system's sensitivity to the fractional order q, demonstrating a clear route to complex dynamics and chaos within a specific range of this parameter.

Fig. 3 includes the bifurcation diagram and entropy analysis, covering the range $a \in [0, 1]$. Although chaotic behavior is exhibited for almost all values of a, in most cases, the system tends to transition from chaotic behavior to periodic behavior after around 500 s. Nevertheless, this system offers a wide range of values for designing a chaotic random number generator based on parameter a.

In particular, the fractional derivative orders impose memory effects and hereditary properties on the system, causing more complex and unpredictable behaviors compared to classical (integer-order) models. The analyses in this section complement studies conducted on integer-order systems and contribute to a deeper understanding of fractional dynamics in curved spacetime under the influence of dark energy.

The present section focuses on the effect of fractional-order derivatives and the normalization constant a on the dynamics of the circular string described in Eq. (1). Three fractional orders, $q_1 = 0.997$, $q_2 = 0.998$, $q_3 = 0.999$, and one integer order $q_4 = 1$ are considered, while keeping the normalization constant fixed at $a = 0.2$. The phase portraits are plotted in the (r, P_r), (r, θ), (r, P_θ), (P_r, θ), (P_r, P_θ), and (θ, P_θ) planes, as shown in Fig. 4. The parameters are set as follows: $\beta = 0.02$, $M = 0.2$, $n = 1$, $a' = 1/\pi$, $l = 15$, $\omega_q = -1/3$, and $P_t = 12$, while the initial conditions are: $r(0) = 10$, $P_r(0) = 2.670855$, $\theta(0) = 0$, and $P_\theta(0) = 5$. Through these six phase portraits, the chaotic characteristics emerging in the radial dynamics of the string system are visualized.

To further analyze the dynamic complexity and spectral characteristics of the system across different orders, Frequency Spectrum (FFT) analysis is performed. Fig. 5 presents the frequency spectra for the integer-order, commensurate fractional-order, and IFO systems. As depicted in Fig. 5a, the integer-order system exhibits a broad and relatively distributed frequency spectrum,

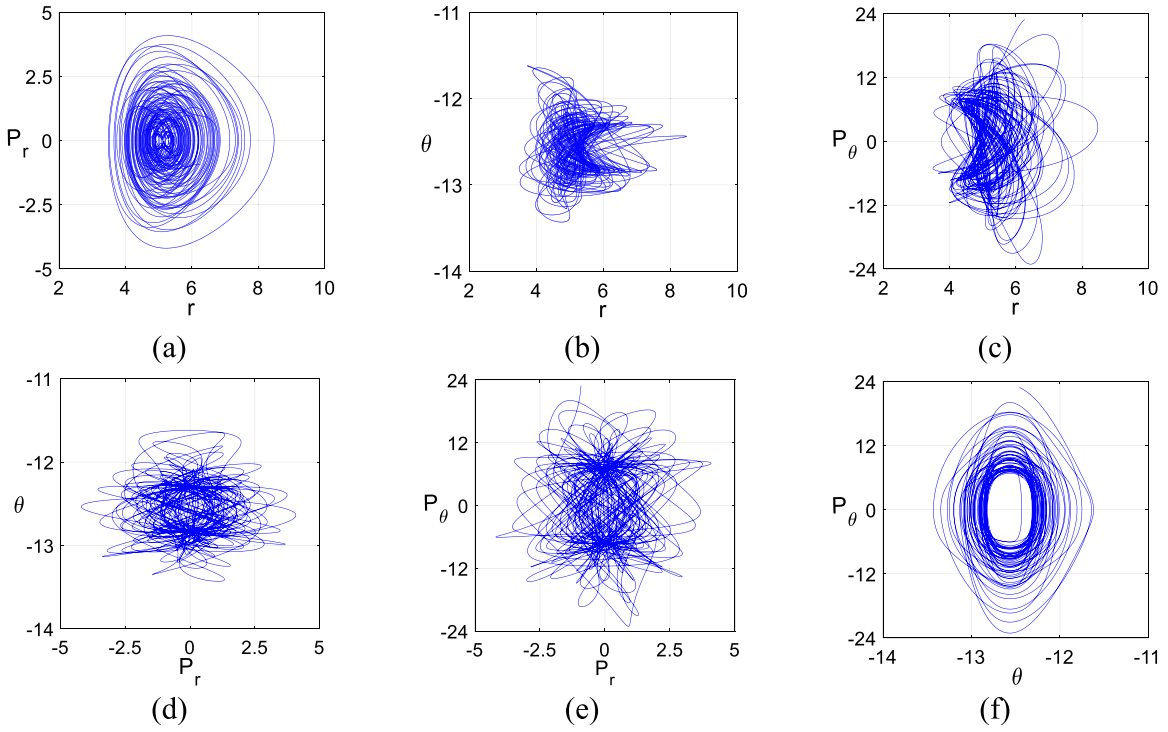

Fig. 4. Chaotic phase portraits of system (1) for the time interval 100–500 s with parameters $q_1 = 0.997$, $q_2 = 0.998$, $q_3 = 0.999$, $q_4 = 1$ and $a = 0.2$.

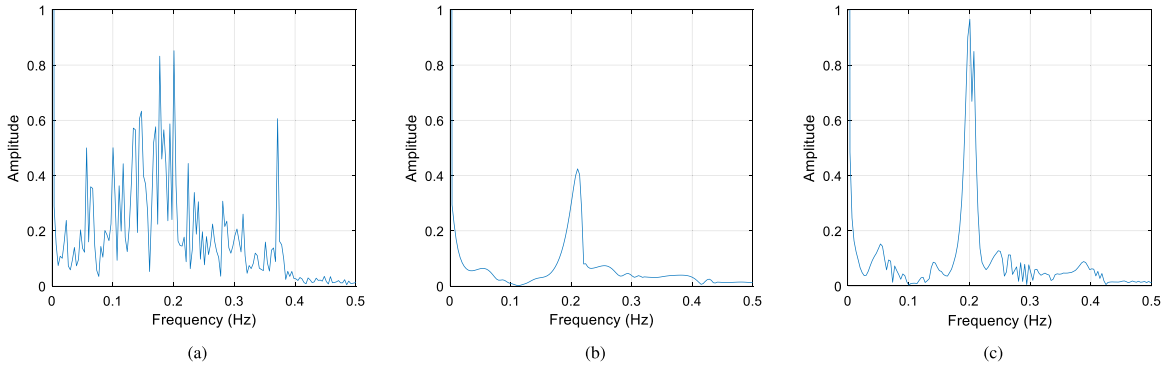

Fig. 5. Frequency spectra (FFT analysis) comparing the complexity of (a) integer-order system (b) commensurate FO system (c) IFO systems.

characteristic of broadband chaotic behavior and indicating a high degree of dynamic complexity. Conversely, Fig. 5b, representing the commensurate fractional-order system, shows a more concentrated frequency distribution with a dominant peak around 0.2 Hz, accompanied by some distributed energy, suggesting a transition towards more organized yet still complex dynamics. Interestingly, Fig. 5c, for the IFO system, displays a pronounced dominant peak at a specific frequency, with its energy highly concentrated. While this indicates a more localized distribution of its dynamic energy in the frequency domain, it does not necessarily diminish its utility for cryptographic purposes. Such concentrated spectral energy can, for instance, be advantageous by potentially simplifying frequency-based synchronization efforts, while the system's inherent sensitivity to initial conditions and long-term unpredictability in its time-domain trajectories, as confirmed by other analyses (e.g., phase portraits and bifurcation diagrams), remain crucial for generating secure chaotic sequences. These FFT analyses collectively provide valuable insights into how the fractional orders influence the system's dynamic energy distribution in the frequency domain.

3. Implementation of the proposed incommensurate fractional-order chaotic system

The PV system is selected as the target application in this study due to several compelling reasons. PV systems are among the most commonly deployed renewable energy sources in smart grid infrastructures, making them a highly relevant and representative case

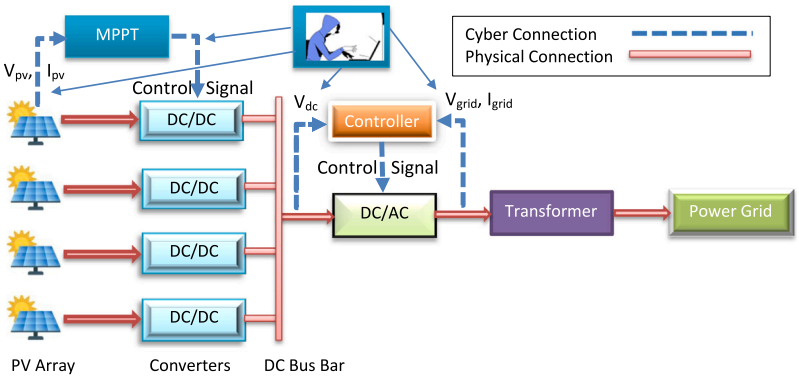

Fig. 6. Description of cyber–physical PV system [10].

study. Furthermore, their exposure to cyber threats, particularly through communication and control links, makes them a critical candidate for evaluating encryption-based countermeasures. In addition, PV systems produce continuous and measurable physical signals (e.g., voltage and current), which are well suited for demonstrating and validating real-time encryption and decryption performance. While this study focuses on PV systems, the proposed encryption framework is designed to be generalizable and can be adapted to other cyber–physical systems such as wind turbines, electric vehicles, and energy storage systems with appropriate modifications.

This section discusses the implementation of the proposed IFO chaotic system as a lightweight encryption scheme for a grid-connected PV system. To achieve this, the cyber–physical PV system is first introduced, and the specific areas where the chaos-based secure communication application is implemented are identified. Then, chaotic sequences are generated from the IFO chaotic system to design a pseudo random number generator (PRNG). These randomly generated numbers are used to encrypt communication signals in the cyber layer of the PV system. In this section, the reliability of the PRNG is validated using the National Institute of Standards and Technology (NIST) tests, and the security of the encryption algorithm is supported by key space, histogram and information entropy analyses.

3.1. Description of cyber–physical PV system

Fig. 6 is a block diagram of a grid-connected PV system, highlighting both its physical and cyber connections. The system consists of multiple PV panels connected in series, each monitored by a Maximum Power Point Tracking (MPPT) controller. The MPPT controller adjusts the duty cycle of the DC–DC converter to extract maximum power, demonstrating a cyber connection through control signals. The DC–DC converters, linked via physical connections, transform the unregulated DC input from the PV panels into a regulated DC voltage suitable for grid integration. This regulated DC voltage is then converted into grid frequency AC voltage by a DC–AC converter (inverter). The inverter's operation is managed by a controller, which receives control signals from a microcontroller through a cyber-connection. To ensure synchronization with the grid and mitigate current harmonics, voltage and current sensors are employed, providing essential feedback for the controller. While traditional systems may use transformers, modern grid-tied inverters often rely on LCL filters instead to reduce size and cost, maintaining system stability and reliability without the need for a transformer. The inclusion of a 'Cyber Attack' symbol in the diagram underscores the system's potential vulnerability to cyber threats, indicating that control signals transmitted over cyber connections could be compromised. Therefore, robust cybersecurity measures are essential in the design and operation of such PV systems. This diagram effectively delineates the primary components, signal flows, and connection types, both physical and cyber, within the PV system.

In this study, the cyber connections shown in Fig. 6 are encrypted using signals from the IFO chaotic system to establish a secure communication network. The encryption process is detailed in Fig. 7a. In this lightweight encryption algorithm, voltage and current signals obtained from power units are masked with random numbers derived from the chaotic system before being transmitted to the receiver. The receiver then performs the decryption process using the same chaotic signals. Note that for the encryption and decryption algorithms to function correctly, both sides must have the same chaotic system running synchronously with identical initial conditions. This requirement, while mathematically sound, poses a significant practical challenge in real-world implementations, particularly in noisy communication environments or large-scale distributed systems. Maintaining precise synchronization and securely distributing these initial conditions (often acting as a cryptographic key) are critical aspects that must be robustly addressed to prevent desynchronization and potential decryption failures. Strategies for mitigating this include employing secure key exchange protocols for initial condition distribution, or exploring adaptive synchronization techniques [40] that can re-establish coupling even with minor discrepancies. This crucial aspect warrants further dedicated research for practical deployment. Fig. 7b illustrates the basic operating principle of the designed cybersecure PV system.

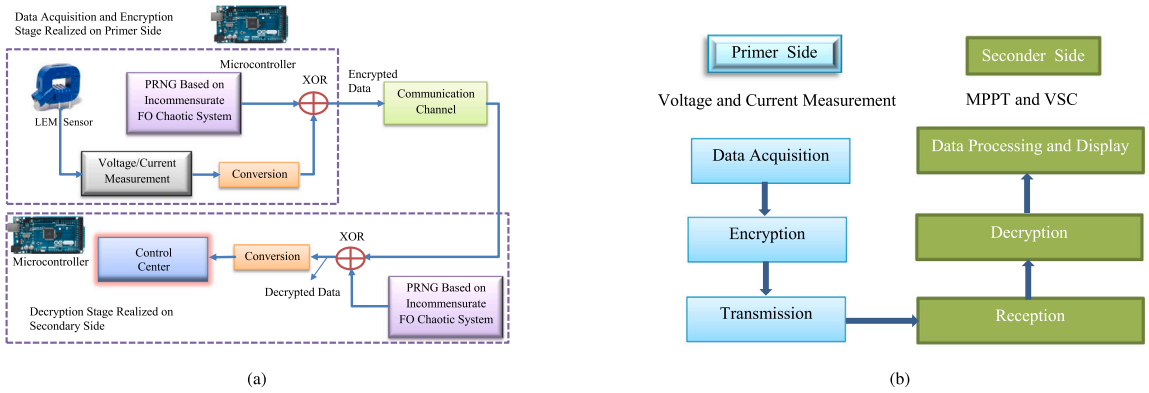

Fig. 7. Encryption-decryption process.

Table 1
P-values from NIST SP800-22 Test Suite.

No	Test type	P-value	Result
01	Frequency (Monobit) Test	0.3843	Pass
02	Frequency Test within a Block	0.6258	Pass
03	Runs Test	0.8956	Pass
04	Longest Run of Ones Test	0.4939	Pass
05	Binary Matrix Rank Test	0.1188	Pass
06	Discrete Fourier Transform (Spectral) Test	0.1299	Pass
07	Non-overlapping Template Matching Test	0.1263	Pass
08	Overlapping Template Matching Test	0.2142	Pass
09	Maurer's Universal Statistical Test	0.3267	Pass
10	Linear Complexity Test	0.7878	Pass
11	Serial Test	0.4859	Pass
12	Approximate Entropy Test	0.6259	Pass
13	Cumulative Sums Test (Forward)	0.7430	Pass
14	Cumulative Sums Test (Backward)	0.4244	Pass
15	Random Excursions Test	0.5754	Pass
16	Random Excursions Variant Test	0.0306	Pass

3.2. Design of PRNG based on incommensurate fractional-order chaotic system

In this study, a new PRNG is developed to encrypt communication signals in the cyber layer of a PV system. The PRNG relies on the time series generated by an IFO chaotic system, which exhibits high sensitivity to initial conditions and system parameters, characteristics essential for cryptographic randomness.

Time series of four state variables (x, y, z, t) are computed using a fractional-order numerical solver ('fde12.m') in MATLAB. After discarding an initial transient, the remaining data is cast into IEEE 754 double-precision floating-point format and typecast into 64-bit unsigned integers. Each 64-bit number is partitioned into four 16-bit blocks, and these blocks are XOR-ed to yield one 16-bit value per variable. These four 16-bit values are then combined through bit-shifting and bitwise OR operations to produce a 64-bit key, denoted as `keyMask`. Each `keyMask` is converted to a 64-bit binary string and saved as a new line in a file named `keyMask_binary.txt`. These binary sequences are later used for encryption and further evaluated through the NIST SP800-22 statistical test suite. The generated sequences successfully passed all 15 standard NIST tests, including Monobit, Block Frequency, Runs, Rank, FFT, Universal Statistical, and more, as well as the Random Excursions and Variant tests. The p-values from each test are provided in Table 1, demonstrating the statistical randomness and unpredictability required for cryptographic use.

3.3. Data acquisition and encryption stage

In the data acquisition stage, voltage and current signals are collected from various monitoring points across the PV system. These signals primarily include outputs from MPPT controllers, DC–DC converters, and inverter units as given in Fig. 1, which represent the cyber–physical interaction of the grid-connected PV infrastructure. The collected data are first pre-processed, filtered and digitized, before being transferred to the encryption unit. Ensuring accurate and timely signal acquisition is crucial, as these data form the basis of the control mechanism and overall energy optimization within the PV system. Any compromise or delay in this communication may lead to system instability or efficiency loss.

Following the data acquisition phase, signal encryption is performed using a lightweight XOR-based method, where a 64-bit pseudo-random key sequence (`keyMask`) is generated from an IFO chaotic system. This approach ensures both computational

efficiency and sufficient cryptographic randomness, making it suitable for real-time embedded systems such as smart grid-connected PV infrastructures.

The keyMask sequence is derived from chaotic variables (x, y, z, t) and saved in 64-bit unsigned integer format. Each sample of the original signal is normalized and typecast into 64-bit format before being XOR-ed with the corresponding element of keyMask, yielding the encrypted data. This one-time pad-like structure provides strong resistance to common cyber attacks, including eavesdropping and man-in-the-middle attacks, due to the entropy and unpredictability of the chaotic PRNG-based key.

The encrypted signal is then transmitted securely through the cyber layer to the control and data processing units. The detailed workflow of the encryption-decryption mechanism is provided in Algorithm 1.

Algorithm 1 Signal Encryption and Decryption using XOR and Chaotic keyMask

Require: Original signal `signal`, chaotic key sequence `keyMask`
Ensure: `encrypted_signal`, `decrypted_signal`

Set $scale \leftarrow 2^{63} - 1$
Normalize input: $signal\_uint64[i] \leftarrow \texttt{uint64}((signal[i] + 1) \cdot scale)$
for $i = 1$ **to** N **do**
    $encrypted\_signal[i] \leftarrow signal\_uint64[i] \oplus keyMask[i]$
end for

— Decryption Phase —
for $i = 1$ **to** N **do**
    $decrypted\_uint64[i] \leftarrow encrypted\_signal[i] \oplus keyMask[i]$
    $decrypted\_signal[i] \leftarrow \texttt{double}(decrypted\_uint64[i])/scale - 1$
end forreturn `encrypted_signal`, `decrypted_signal`

3.4. Decryption stage and data processing

In the decryption stage, the encrypted signals received by the control and monitoring system are processed using the same 64-bit pseudo-random sequence (keyMask) that was employed during the encryption phase. Since the XOR operation is symmetric and self-inverting, applying the XOR operation again between each encrypted sample and its corresponding keyMask element accurately restores the original signal.

To maintain security and synchronization, both the transmitter and receiver utilize identical chaotic key generators initialized with the same fractional-order parameters and initial conditions. This ensures the generation of an identical keyMask sequence on both ends of communication.

The decryption process, as described in Algorithm 1, begins by performing a bitwise XOR operation on the encrypted 64-bit integers with the generated key sequence. The resulting values are then normalized back into their original range (e.g., $[-1, 1]$ for a sinusoidal signal), to reconstruct the continuous-time voltage or current signal. As all data are transmitted in raw 64-bit format, no information is lost during this transformation.

This lightweight, reversible method not only ensures data confidentiality but also preserves the signal's integrity with minimal computational overhead, making it ideal for real-time embedded PV monitoring systems.

3.5. Numerical test of encryption-decryption algorithm

The encryption and decryption process was visually evaluated using the generated sine wave signal. The encryption algorithm applies a bitwise XOR operation on the signal using a PRNG-based key mask. The three different signals shown in Fig. 8 demonstrate the effectiveness and accuracy of the processes. The original signal (blue line) is smooth and continuous, which is typical of a sine wave with a frequency of 5 Hz and a sampling rate of 1000 Hz. The encrypted signal (red dashed line) shows significant distortion and appears as random noise, indicating that the encryption algorithm effectively obscures the original information and ensures its security. The decrypted signal (green dash-dotted line) closely matches the original signal, demonstrating that the decryption process, using the same key mask, successfully restores the original signal with high accuracy. Any small discrepancies may arise from data type conversions or precision limitations in floating-point operations. In addition to the visual evaluation, several performance analyses are conducted in subsections to assess the robustness and security of the encryption algorithm. These analyses confirm that the algorithm is both secure and effective in maintaining the integrity of the original signal during encryption and decryption.

4. Evaluation of the designed encryption-decryption method

As shown in Fig. 9, the 100-kW grid-connected PV array is modeled to operate with high efficiency and stability under varying environmental conditions. The PV system delivers up to 100 kW at 1000 W/m^2 irradiance and is interfaced with the grid via a 5-kHz DC–DC boost converter and a three-phase, three-level Voltage Source Converter (VSC). The MPPT controller, implemented in Simulink using the Perturb and Observe technique, dynamically adjusts the duty cycle of the boost converter to extract maximum power from the PV array. The boost converter increases the PV voltage from its natural maximum power point level of approximately 272 V DC to a regulated 500 V DC output.

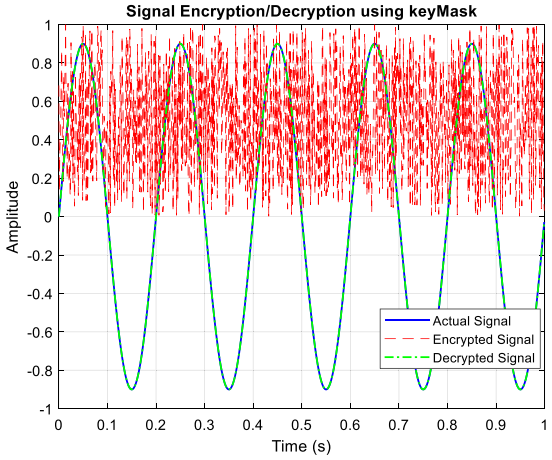

Fig. 8. Actual, encrypted and decrypted signals using the Algorithm 1.

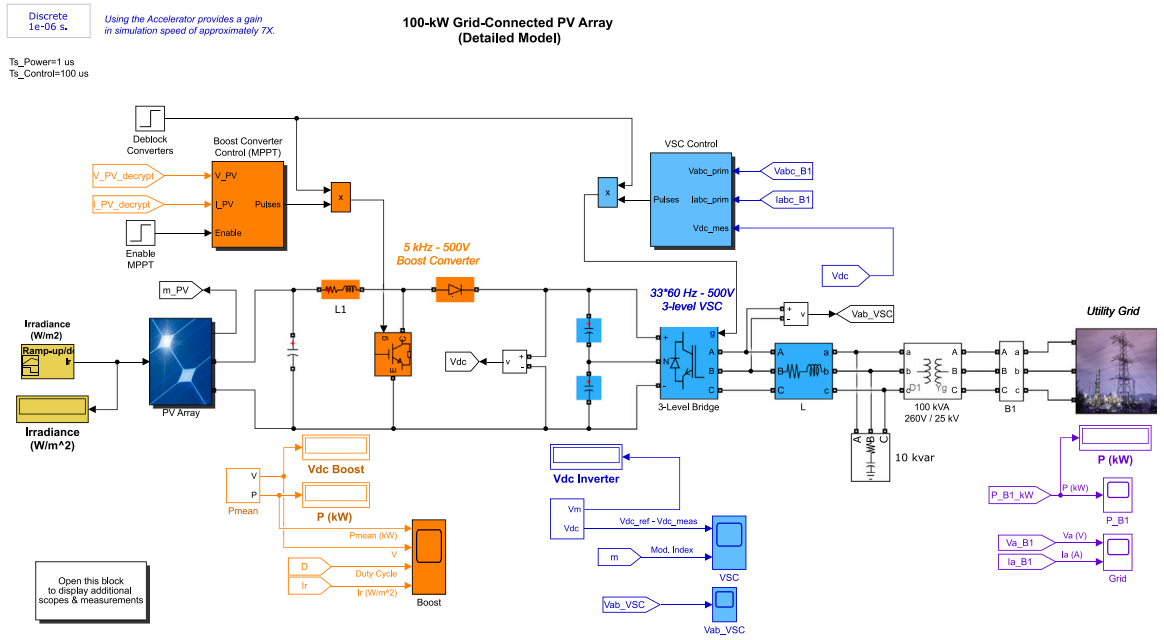

Fig. 9. Matlab/Simulink model of the PV system [41].

The regulated DC output is then converted to a 260 V AC, 60-Hz signal through a three-phase, 3-level VSC, which is optimized to maintain unity power factor. The VSC operation is governed by Pulse Width Modulation (PWM) techniques, and the control is supported by a Phase-Locked Loop (PLL) to ensure precise synchronization with the grid frequency. To mitigate harmonics generated by the VSC, a 10-kVAR capacitor bank is connected to the output, improving power quality. The AC output is stepped up through a 100-kVA, 260 V/25 kV three-phase transformer before being injected into the utility grid, which is modeled as a 25-kV distribution feeder coupled with a 120-kV equivalent transmission system. The model operates with a discretization of 1 μs for the power electronics components and 100 μs for the control algorithms, providing high-fidelity simulation results. The entire MATLAB/Simulink model was designed by Giroux and is provided in [41].

In this study, the signals within the cyber layer of this model are encrypted using the proposed method, as detailed in Section 3. The voltage and current signals obtained from the PV panels are encrypted as described in Algorithm 1 and then sent to the MPPT block. Here, decryption is applied to obtain the actual signals, and these decrypted signals are used in the Perturb and Observe method. Using the MPPT algorithm, a control signal is generated to drive the boost converter. On the other hand, V_{dc} (bus voltage) is also encrypted in a similar manner, and these encrypted signals are sent to the Voltage Source Control block of the inverter. The decrypted V_{dc} signal is used here to control the inverter.

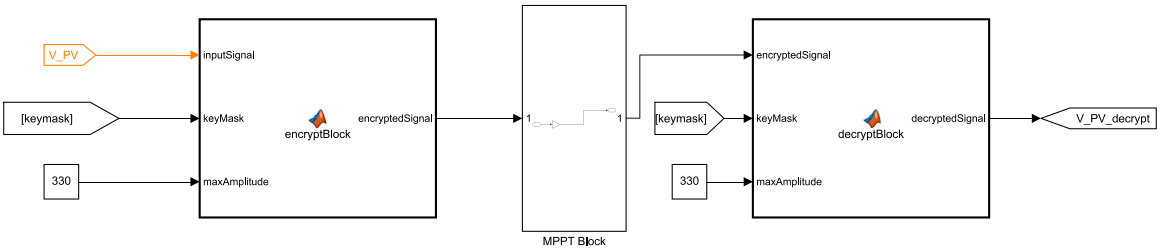

Fig. 10. Encryption-decryption algorithm designed in Matlab/Simulink.

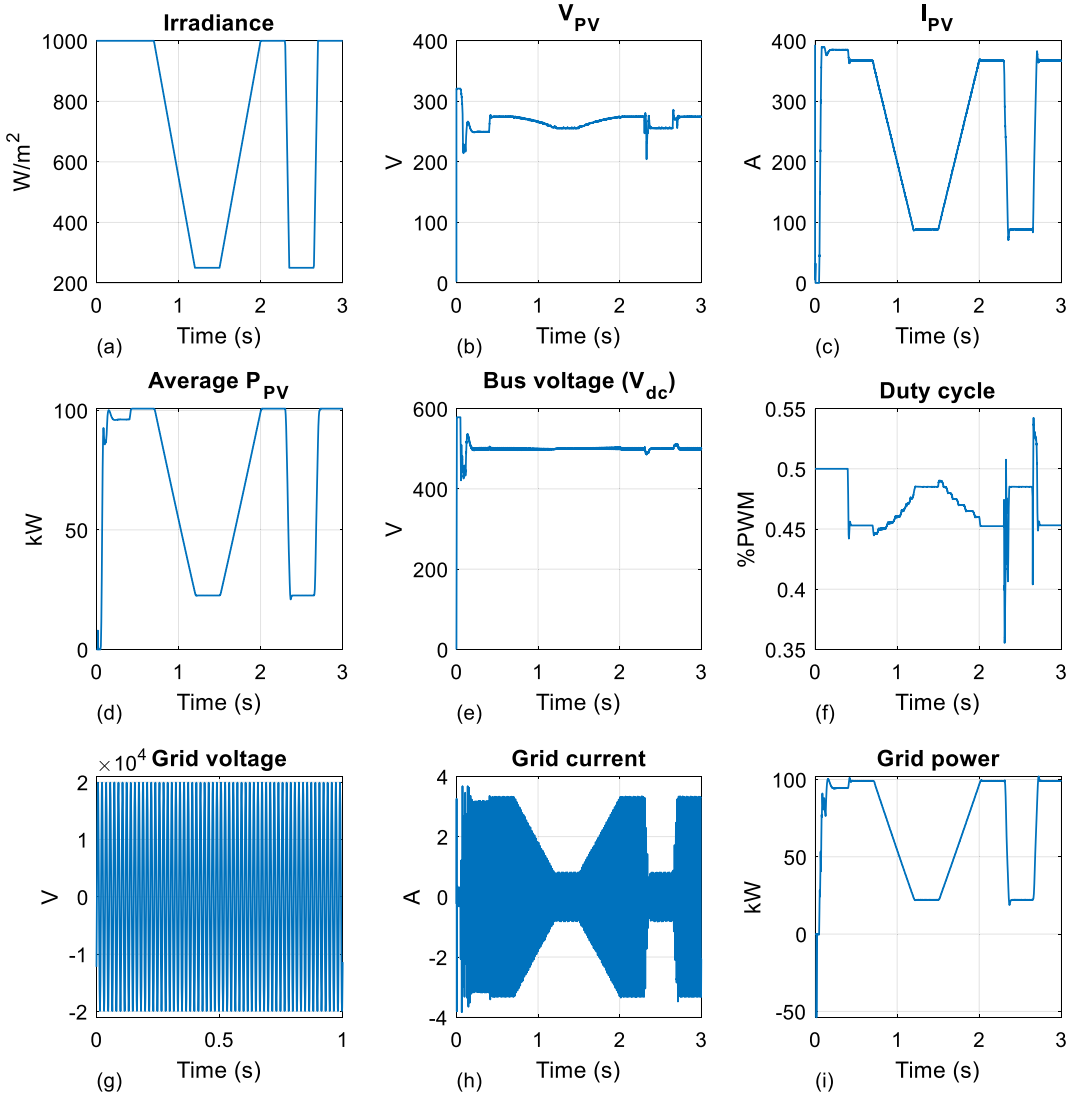

Fig. 11. Measurements from PV system without encryption–decryption algorithm.

The encryption/decryption part of this simulation, which was carried out in the Matlab/Simulink environment, is designed as shown in Fig. 10. In this design, using Simulink function blocks, the previously generated random key is retrieved from memory, and a different random number is used at each sampling time to enhance the robustness of the encryption. The contents of the functions shown in Fig. 10 can be found in the Appendix.

Fig. 11 illustrates the dynamic behavior of the simulated PV system operating without the encryption–decryption algorithm. As shown in Fig. 11a, the irradiance varies significantly over the 3-second simulation period, dropping as low as 200 W/m^2 and

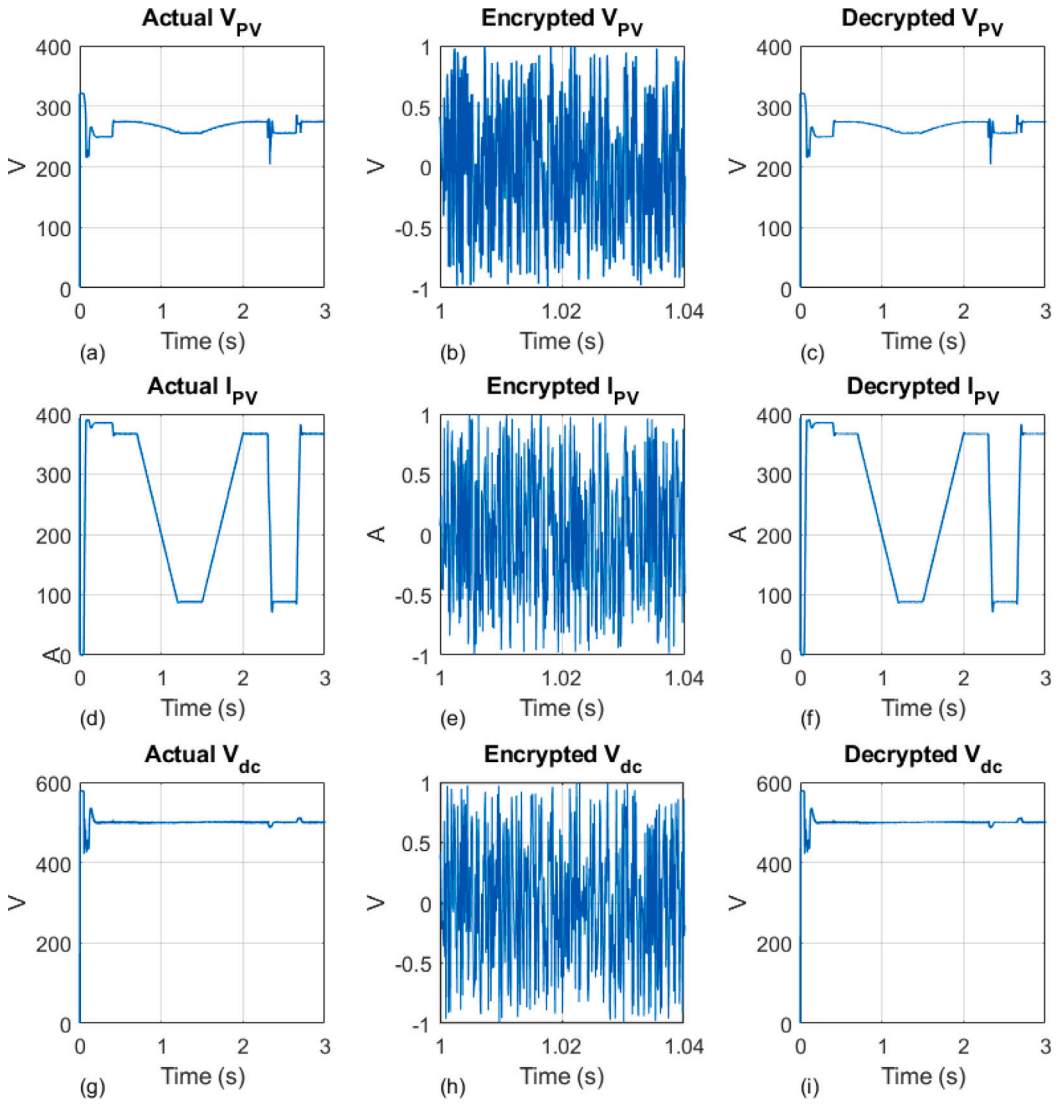

Fig. 12. Encrypted–decrypted measurements.

returning to full irradiance (1000 W/m^2), thereby testing the robustness of the MPPT algorithm under realistic environmental fluctuations. Correspondingly, the PV voltage (Fig. 11b) and current (Fig. 11c) show appropriate responses to these changes, with the MPPT controller adjusting the duty cycle (Fig. 11f) of the boost converter to track the maximum power point.

The effect of irradiance fluctuations is also reflected in the average power output of the PV array (Fig. 11d) and the bus voltage V_{dc} (Fig. 11e), where the latter remains relatively stable around 500 V due to the boost converter's regulation. Notably, the inverter-side parameters, including the grid voltage (Fig. 11g), grid current (Fig. 11h), and grid power (Fig. 11i), confirm successful grid synchronization and power injection. The sinusoidal waveform in (Fig. 11g) indicates proper grid voltage, while the current waveform (Fig. 11h) adjusts in amplitude with available PV power, showing reduced current during low irradiance intervals. In Fig. 11i, grid power closely tracks the PV power output, confirming effective power transfer and minimal losses.

Then, the system is executed using the designed encryption-decryption algorithm. As illustrated in Fig. 12, three different signal types, V_{PV}, I_{PV} and V_{dc} are encrypted and then decrypted to evaluate the performance of the proposed scheme. The actual measurements (Figs. 12a, d, g) reflect the original measured data. Once encrypted (Figs. 12b, e, h), the signals appear completely unintelligible and effectively masked, demonstrating that the encryption process successfully hides the information content from unauthorized access.

As shown in Figs. 12c, f, and i, the original signals are successfully recovered after decryption with high accuracy, indicating that any data loss during transmission and processing was minimal or negligible. The decrypted signals closely match the original ones in both amplitude and shape, which highlights the reliability and precision of the encryption-decryption process. These findings demonstrate that the proposed algorithm maintains data confidentiality during transmission without compromising the quality or

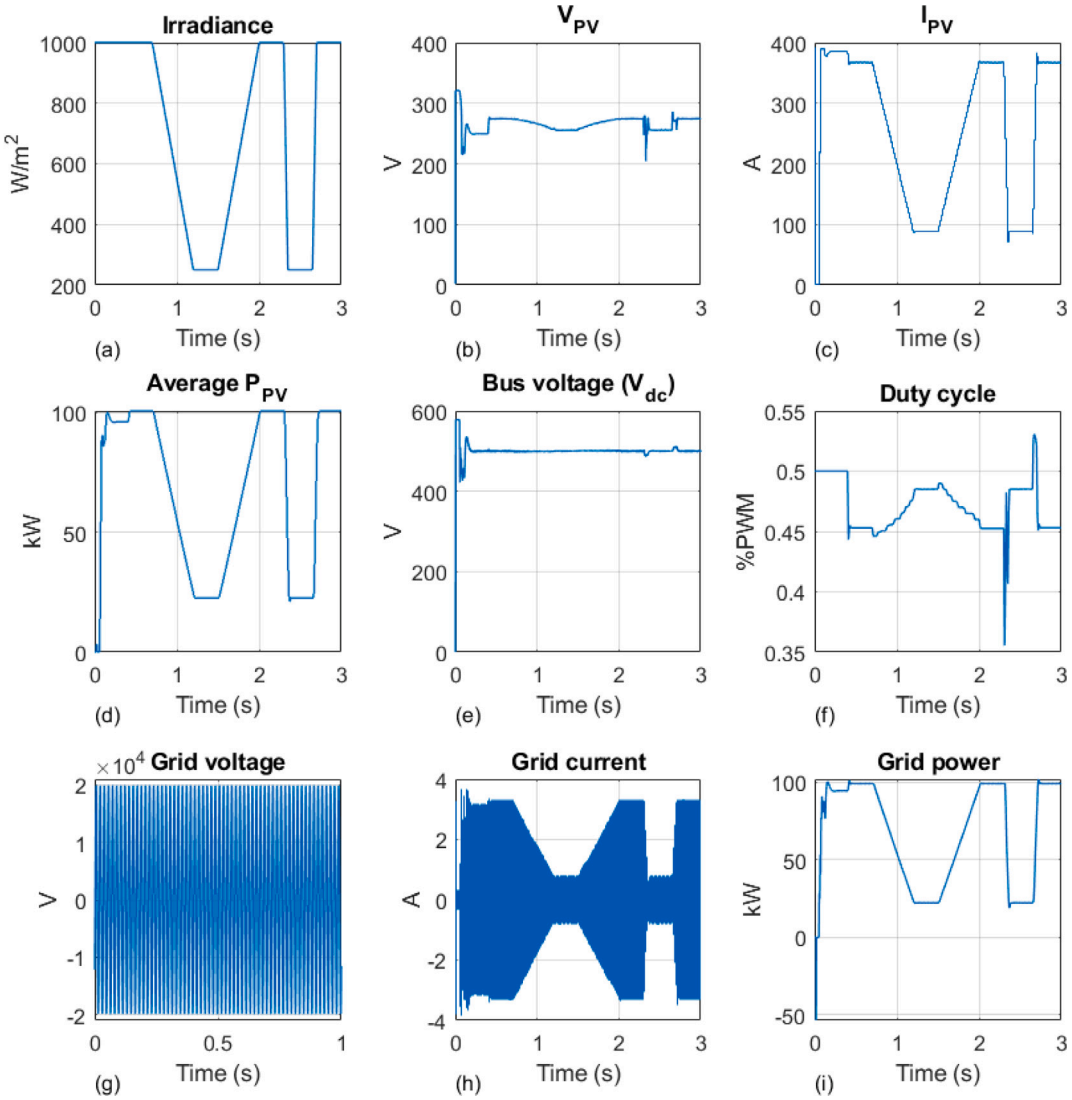

Fig. 13. Measurements from PV system with encryption-decryption algorithm.

accuracy of the original measurements. Fig. 13 presents the system performance while the encryption-decryption algorithm is active in the simulation. Although the communication channel carries signals that appear random (Figs. 12b, e, h), the grid power still closely follows the PV power output as shown in Fig. 13i. This confirms the proper functioning of both the MPPT (Fig. 13b, c, d) and VSC systems (Fig. 13e, f, g, h). The robustness of the encryption-decryption method is further analyzed in the following subsection.

It is important to note some limitations of the proposed encryption-decryption algorithm. The encryption process introduces a certain amount of time delay, which is detectable even in the simulation environment and may impact real-time system responsiveness. Furthermore, the use of an IFO chaotic system inherently demands greater memory resources from the microcontroller due to its computational complexity. This necessitates the employment of more advanced microcontrollers with higher processing power and memory capacity, which may increase the overall system cost and complexity.

4.1. Performance evaluation of encryption-decryption algorithm

In addition to the visual evaluation, several performance analyses are conducted in subsections to assess the robustness and security of the encryption algorithm. These analyses confirm that the algorithm is both secure and effective in maintaining the integrity of the original signal during encryption and decryption.

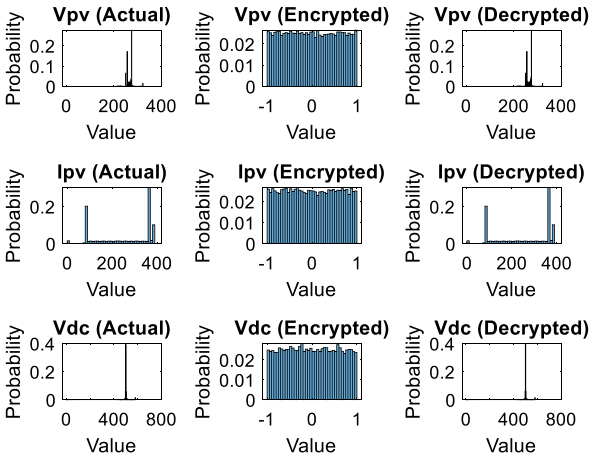

Fig. 14. Histograms of actual, encrypted, and decrypted signals for V_{PV}, I_{PV}, and V_{dc}.

4.1.1. Key space analysis

In the analysis of the key space, the robustness of the encryption algorithm is examined in terms of the size and complexity of the key space. A larger key space generally means greater security (keyspace of 2^{100} can be considered computationally secure [42]), as it becomes computationally more difficult for an attacker to attempt a brute force attack. In this study, the key space of the proposed chaotic system-based encryption algorithm is evaluated by analyzing the total number of possible keys. Each parameter and initial condition in the 4D IFO chaotic system (a, M, n, a', l, ωq, Pt, $r(0)$, $Pr(0)$, $\theta(0)$, $P_\theta(0)$, q_1, q_2, q_3, q_4) is represented using IEEE 754 floating-point format, which allows approximately 10^{14} distinguishable values per parameter within practical ranges. As a result, the total key space of the proposed lightweight encryption scheme is approximately $10^{210} \approx 2^{697}$, which is sufficiently large to resist brute-force attacks.

4.1.2. Histogram analysis

To get a better understanding of how well the encryption works, histograms of the actual, encrypted, and decrypted signals for V_{PV}, I_{PV}, and V_{dc} are given. In a secure encryption scheme, the encrypted data should look like random noise, completely uniform with no obvious patterns [43]. As shown in Fig. 14, the first column shows the histograms of the original signals. These have clear spikes and patterns, which is expected since real-world data is not random. The second column shows what happens after encryption. The histograms are almost perfectly flat and spread evenly between −1 and 1, which means the encryption is successfully removed any traces of the original structure. Finally, the third column displays the decrypted signals. These histograms closely resemble the originals, indicating that the decryption process is accurate and do not lose any important information. Overall, the histogram results show that the encryption algorithm is effective in masking the original data.

4.1.3. Information entropy

Information entropy is a fundamental concept from information theory that quantifies the amount of uncertainty or randomness in a dataset. In the context of cryptography, high entropy in encrypted data indicates that the signal behaves like random noise, making it more resistant to pattern-based attacks. Mathematically, the Shannon entropy H of a discrete signal is defined as:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{4}$$

where p_i is the probability of the ith symbol or value occurring in the dataset, and the sum is taken over all n unique bins (typically from a histogram of the signal). Higher entropy values suggest a more uniform distribution, which is ideal for ciphertexts, as it implies no predictable structure remains.

In this study, entropy is calculated for three key signals, V_{PV}, I_{PV}, and V_{dc}, in their original (actual), encrypted, and decrypted forms. Each signal is discretized using histogram binning, and entropy was computed from the normalized probability distribution. The calculated results are as follows:

- V_{PV}: Actual entropy = 4.0931, Encrypted = 5.3213, Decrypted = 4.0931
- I_{PV}: Actual entropy = 3.7898, Encrypted = 5.3211, Decrypted = 3.7898
- V_{dc}: Actual entropy = 2.3404, Encrypted = 5.3207, Decrypted = 2.3404

As shown above, the encrypted signals consistently exhibit significantly higher entropy values, close to the maximum for the range used, demonstrating the effectiveness of the encryption algorithm in generating a randomized ciphertext. Just as importantly, the decrypted signals return exactly to their original entropy values, confirming the accuracy and reversibility of the encryption process with no data loss. This analysis confirms that the algorithm both obscures patterns successfully and preserves the original data integrity upon decryption, which are essential qualities for the masking algorithm.

5. Conclusion

In this study, an encryption framework aimed at strengthening the cybersecurity of PV systems integrated within smart grid environments is introduced. Unlike conventional approaches, the designed method targets the masking of signals, using a chaos-based encryption scheme inspired by concepts from theoretical physics. Specifically, the encryption algorithm is built upon the IFO dynamics of strings around the Bardeen-AdS black hole surrounded by quintessence dark energy. This innovative blend of cosmological modeling and fractional calculus allows for the generation of highly complex, unpredictable chaotic sequences, ideal for secure data transmission.

Simulations carried out on a grid-connected PV system in Matlab/Simulink confirm the effectiveness of the approach. The encrypted signals display nearly uniform histogram distributions and elevate information entropy levels, both strong indicators of cryptographic robustness. More importantly, the decryption process perfectly recovers the original signals, maintaining data integrity without any loss.

This work demonstrates that advanced mathematical models from areas like high-energy physics and cosmology can be successfully applied to real-world cybersecurity challenges. It also underscores the powerful potential of chaos theory in protecting cyber–physical energy systems. By implementing this method, PV systems, key players in the transition to sustainable energy, can operate securely even in highly interconnected and increasingly vulnerable digital infrastructures.

However, it should be noted that while the proposed XOR-based encryption architecture offers inherent lightness, the integration of IFO chaotic dynamics inherently introduces computational overhead. This results in increased computation time and greater memory and processing requirements for the microcontroller, necessitating more advanced hardware. These factors may affect real-time responsiveness and increase the cost and complexity of practical implementations. Therefore, a careful trade-off between enhanced security provided by the complex dynamics and the computational demands for real-time deployment is essential. Furthermore, the inherent reliance on precise initial synchronization of chaotic systems between transmitter and receiver presents a practical challenge, as minor discrepancies or communication delays can lead to desynchronization and impede accurate decryption.

Future research will specifically focus on optimizing the computational efficiency of the fractional-order chaotic system for real-time deployment on embedded hardware. This will involve exploring hardware-accelerated implementations, simplified numerical solvers, and dedicated cryptographic hardware architectures to mitigate the identified delays and memory demands. Furthermore, we will assess its scalability across broader applications, including smart grids, distributed energy resources, and IoT-based energy networks.

CRediT authorship contribution statement

Haris Calgan: Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization, Funding acquisition. **Abdullah Gokyildirim:** Writing – original draft, Data curation, Investigation, Formal analysis, Software, Methodology. **Suleiman M. Sharkh:** Validation, Supervision, Writing – review & editing. **Metin Demirtas:** Validation, Software, Conceptualization, Supervision, Writing – review & editing.

Acknowledgments

This study was funded by Scientific Research Projects Unit of Balikesir University, Turkey under the project no BAP 2024/022. H.C. thanks the TUBITAK BIDEB-2219 program for a postdoctoral grant (1059B192400296). The authors also thank Berkay Emin for the useful discussion.

Appendix A. MATLAB encryption function code

```
function encryptedSignal = encryptBlock(inputSignal, keyMask, maxAmplitude)
%#codegen

persistent idx

if isempty(idx)
    idx = 1;
end

if idx > length(keyMask)
    idx = 1;
end

range = 2 * maxAmplitude;
scale = floor(2^64 / range);

% Scaling and shifting
signal_uint64 = uint64((inputSignal + maxAmplitude) * scale);
% [-A,+A] -> [0, 2^64-1]
```

```
% XOR operation
mask = keyMask(idx);
encUint = bitxor(signal_uint64, mask);

% Output
encryptedSignal = double(encUint);

% Update counter
idx = idx + 1;
```

Listing 1 encryptBlock function used in encryption process

Appendix B. MATLAB decryption function code

```
function decryptedSignal = decryptBlock(encryptedSignal, keyMask, maxAmplitude)
%#codegen

persistent idx

if isempty(idx)
    idx = 1;
end

if idx > length(keyMask)
    idx = 1;
end

range = 2 * maxAmplitude;
scale = floor(2^64 / range);

% XOR
encUint = uint64(encryptedSignal);
mask = keyMask(idx);
origUint = bitxor(encUint, mask);

% Undo scaling
scaledOutput = double(origUint);
decryptedSignal = (scaledOutput / scale) - maxAmplitude;

% Increment counter
idx = idx + 1;
```

Listing 2 decryptBlock function used in decryption process

Data availability

Data will be made available on request.

References

[1] M.A.I. Rafi, M.S. Hasan, M.M. Hasan, J.A. Chowdhury, M.R. Sohan, N.A. Jahan, M.M. Hossain, et al., Techno-economic and environmental analysis of solar pv system at sher-e-bangla national cricket stadium: A comprehensive case study, IEEE Access (2025).

[2] B. Arbab-Zavar, S.M. Sharkh, E.J. Palacios-Garcia, J.C. Vasquez, J.M. Guerrero, Reducing detrimental communication failure impacts in microgrids by using deep learning techniques, Sensors 22 (16) (2022) 6006.

[3] M. Shaaban, U. Tariq, M. Ismail, N.A. Almadani, M. Mokhtar, Data-driven detection of electricity theft cyberattacks in pv generation, IEEE Syst. J. 16 (2) (2021) 3349–3359.

[4] S. Jadidi, H. Badihi, Y. Zhang, Active cyber-resilient control for a pv system at microgrid level, in: 2021 IEEE 4th International Conference on Renewable Energy and Power Engineering, REPE, IEEE, 2021, pp. 339–344.

[5] L. Guo, J. Zhang, J. Ye, S.J. Coshatt, W. Song, Data-driven cyber-attack detection for pv farms via time-frequency domain features, IEEE Trans. Smart Grid 13 (2) (2021) 1582–1597.

[6] V.S. Rajkumar, A. Ştefanov, A. Presekal, P. Palensky, J.L.R. Torres, Cyber attacks on power grids: Causes and propagation of cascading failures, IEEE Access 11 (2023) 103154–103176.

[7] D.E. Whitehead, K. Owens, D. Gammel, J. Smith, Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, in: 2017 70th Annual Conference for Protective Relay Engineers, CPRE, IEEE, 2017, pp. 1–8.

[8] A. Walker, J. Desai, D. Saleem, T. Gunda, Cybersecurity in photovoltaic plant operations, in: National Renewable Energy Lab, Tech. rep., NREL, Golden, CO (United States, 2021.
[9] J. Zhang, Q. Li, J. Ye, L. Guo, Cyber-physical security framework for photovoltaic farms, in: 2020 IEEE CyberPELS (CyberPELS), IEEE, 2020, pp. 1–7.
[10] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, H.A. Mantooth, Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network, IEEE Trans. Power Electron. 36 (3) (2020) 2495–2498.
[11] J. Kim, H. Ibrahim, S. Wang, A. Mete, L. Xie, P. Enjeti, P. Kumar, Cyber-secure and safe operation of solar photovoltaic power distribution systems, in: 2024 IEEE Applied Power Electronics Conference and Exposition, APEC, IEEE, 2024, pp. 1280–1287.
[12] M. Dayarathne, M. Jayathilaka, R. Bandara, V. Logeeshan, S. Kumarawadu, C. Wanigasekara, Mitigating cyber risks in smart cyber–physical power systems through deep learning and hybrid security models, IEEE Access (2025).
[13] R. Subramaniam, A.J. Sheela, A. Alwabli, Enhanced cybersecurity and cyber-attack detection in smart dc micro grids using blockchain technology and svm technique, Ain Shams Eng. J. 16 (7) (2025) 103400.
[14] S. Tufail, H. Iqbal, M. Tariq, A. Sarwat, A hybrid machine learning-based framework for data injection attack detection in smart grids using pca and stacked autoencoders, IEEE Access (2025).
[15] P. Biswas, A. Rashid, A. Al Masum, M.A. Al Nasim, A.A. Ferdous, K.D. Gupta, A. Biswas, An extensive and methodical review of smart grids for sustainable energy management-addressing challenges with ai, Renew. Energy Integr. Leading- Edge Technol. IEEE Access (2025).
[16] E. Vignesh, P. Aruna Jeyanthy, Efficient and secure integration of renewable energy sources in smart grids using hybrid fuzzy neural network and improved diffie-hellman key management, Comput. Electr. Eng. 123 (2025) 110206, http://dx.doi.org/10.1016/j.compeleceng.2025.110206, https://www.sciencedirect.com/science/article/pii/S0045790625001491.
[17] F. Harrou, B. Taghezouit, B. Bouyeddou, Y. Sun, Cybersecurity of photovoltaic systems: challenges, Threat. Mitig. Strat.: A Short Surv. Front. Energy Res. 11 (2023) 1274451.
[18] V. Vismaya, S.S. Muni, A.K. Panda, B. Mondal, Degn–harrison map: Dynamical and network behaviours with applications in image encryption, Chaos Solitons Fractals 192 (2025) 115987.
[19] T. Haridas, S. Upasana, G. Vyshnavi, M.S. Krishnan, S.S. Muni, Chaos-based audio encryption: Efficacy of 2d and 3d hyperchaotic systems, Frankl. Open 8 (2024) 100158.
[20] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, A. Istanbullu, Chaos-based engineering applications with a 3d chaotic system without equilibrium points, Nonlinear Dynam. 84 (2016) 481–495.
[21] B. Emin, M. Yaz, Digital implementation of chaotic systems using nvidia jetson agx orin and custom dac converter, Chaos Fractals 1 (1) (2024) 38–41.
[22] L. Liu, Research on smart grid data encryption algorithm based on new complex chaotic system, J. Comput. Methods Sci. Eng. (2025) 14727978251346081.
[23] B. Vaseghi, M.A. Pourmina, S. Mobayen, Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control, Nonlinear Dynam. 89 (2017) 1689–1704.
[24] M. Demirtas, S.M. Sharkh, A. Gokyildirim, H. Calgan, Secure operation of a stand-alone wind energy system based on an incommensurate fractional-order chaotic system, Appl. Energy 384 (2025) 125477.
[25] H. Li, Y. Shen, Y. Han, J. Dong, J. Li, Determining lyapunov exponents of fractional-order systems: A general method based on memory principle, Chaos Solitons Fractals 168 (2023) 113167.
[26] S.S. Muni, Ergodic and resonant torus doubling bifurcation in a three-dimensional quadratic map, Nonlinear Dynam. 112 (6) (2024) 4651–4661.
[27] S. Iqbal, J. Wang, A novel fractional-order 3-d chaotic system and its application to secure communication based on chaos synchronization, Phys. Scr. 100 (2) (2025) 025243.
[28] H. Calgan, Incommensurate fractional-order analysis of a chaotic system based on interaction between dark matter and dark energy with engineering applications, Phys. A 635 (2024) 129490.
[29] H. Li, J. Li, H. Fei, G. Hong, J. Dong, A. Yu, Chaotic dynamics of granules-beam coupled vibration: Route and threshold, Mech. Syst. Signal Process. 218 (2024) 111555.
[30] J. Xie, Y. Wang, B. Tang, Chaotic dynamics of strings around the bardeen-ads black hole surrounded by quintessence dark energy, Phys. the Dark Universe 40 (2023) 101184.
[31] E. Ayón-Beato, A. Garcıa, The bardeen model as a nonlinear magnetic monopole, Phys. Lett. B 493 (1–2) (2000) 149–152.
[32] F. Nascimento, P.H. Morais, J. Toledo, V. Bezerra, Some remarks on bardeen-ads black hole surrounded by a fluid of strings, Gen. Relativity Gravitation 56 (7) (2024) 86.
[33] V. Kiselev, Quintessence and black holes, Classical Quantum Gravity 20 (6) (2003) 1187.
[34] P. Basu, P. Chaturvedi, P. Samantray, Chaotic dynamics of strings in charged black hole backgrounds, Phys. Rev. D 95 (6) (2017) 066014.
[35] R. Garrappa, On linear stability of predictor–corrector algorithms for fractional differential equations, Int. J. Comput. Math. 87 (10) (2010) 2281–2290.
[36] R. Garrappa, Predictor–corrector pece method for fractional differential equations, MATLAB Central File Exch. Retrieved April. 26 (2025) 2025, https://www.mathworks.com/matlabcentral/fileexchange/32918-predictor–corrector-pece-method-for-fractional-differential-equations.
[37] A. Kaveh, M. Vahedi, M. Gandomkar, Improving the performance of a chaotic nonlinear system of fractional-order brushless direct current electric motor using fractional-order sliding mode control, An Int. J. Optim. Control.: Theor. Appl. (2025) 8407, http://dx.doi.org/10.36922/ijocta.8407.
[38] F. Evirgen, E. Uçar, N. Özdemir, E. Altun, T. Abdeljawad, The impact of nonsingular memory on the mathematical model of hepatitis c virus, Fractals 31 (04) (2023) 2340065.
[39] E. Uçar, S. Uçar, F. Evirgen, N. Özdemir, Investigation of e-cigarette smoking model with mittag-leffler kernel, Found. Comput. Decision Sci. 46 (01) (2021).
[40] I. Ahmad, A.B. Saaban, A.B. Ibrahim, S. Al-Hadhrami, M. Shahzad, S.H. Al-Mahrouqi, A research on adaptive control to stabilize and synchronize a hyperchaotic system with uncertain parameters, An Int. J. Optim. Control.: Theor. Appl. (IJOCTA) 5 (2) (2015) 51–62.
[41] P. Giroux, Grid-connected pv array, 2025, p. 2025, https://www.mathworks.com/matlabcentral/fileexchange/34752-grid-connected-pv-array, mATLAB Central File Exchange. Retrieved April 6.
[42] S. Iqbal, J. Wang, H. Calgan, Fractional chaotic dynamics in the rucklidge system and its application to image encryption, Nonlinear Dynam. (2025) 1–25.
[43] B. Emin, A. Akgul, F. Horasan, A. Gokyildirim, H. Calgan, C. Volos, Secure encryption of biomedical images based on arneodo chaotic system with the lowest fractional-order value, Electronics 13 (11) (2024) 2122.