energies

MDPI

Article

Irradiance-Driven Natural Watermarking for Detection of False Data Injection in PV Inverters

Lars Bjorndal, Imasha Balahewa, Naser Vosoughi Kurdkandi, Tong Huang * and Chris Mi

Department of Electrical and Computer Engineering, San Diego State University, 5500 Campanile Drive, San Diego, CA 92182, USA; lbjorndal@sdsu.edu (L.B.); ibalahewa@sdsu.edu (I.B.); nvosoughikurdkandi@sdsu.edu (N.V.K.); cmi@sdsu.edu (C.M.)

* Correspondence: thuang7@sdsu.edu

Abstract

The widespread deployment of photovoltaic (PV) inverters with digital control and communication systems has increased the power grid's attack surface, making it more vulnerable to cyberattacks. This creates a need for locally implementable attack-detection methods that do not disrupt inverter operation. This paper therefore proposes an irradiance-driven natural watermarking approach for decentralized detection of false data injection (FDI) attacks on inverter terminal measurements. The approach leverages irradiance-driven DC-link voltage variations to watermark the inverter outputs, generating a non-removable signature in the true measurements. The proposed method is evaluated using a real-time hardware-in-the-loop model of a three-phase grid-following PV inverter that captures PV-array and grid-connection dynamics. Implementation robustness is further assessed on a separate hardware grid-forming inverter testbed with non-idealized components. In the tested cases, the detection model identifies noise-injection and replay attacks within 15 ms, while otherwise undetectable model-based attacks are revealed when DC-link voltage variations between 5% and 10% occur. These experimental results demonstrate that irradiance-driven natural watermarking can reveal FDI attacks without affecting normal inverter operation.

Keywords: cyber–physical systems; cybersecurity; false data injection; grid-tied inverter; natural watermarking; photovoltaic power systems

1. Introduction

The rise in renewable energy deployment significantly expands the attack surface of the power grid [1]. Power generation has traditionally been dominated by large synchronous generators, and cybersecurity efforts have therefore primarily focused on securing these generators and the surrounding transmission and distribution infrastructure. However, the low geographic power density of wind and solar generation requires larger land areas per unit of energy produced, resulting in a much larger number of distributed generation units [2]. These renewable generation units interface with power grids through power electronic inverters with digital sensing, control, and communication systems, making them vulnerable to cyberattacks and motivating the need for novel detection solutions.

This increased vulnerability of renewables reflects a broader trend in the security risks facing industrial control systems (ICSs). Although ICSs were once considered secure because of their isolation and specialized software, the 2010 Stuxnet attack on Iran's uranium enrichment facilities exposed their potential vulnerabilities [3]. Since then, the increasing

Received: 12 May 2026
Revised: 9 June 2026
Accepted: 12 June 2026
Published: 16 June 2026

digitalization of ICSs and remote access capabilities has been paralleled by a growing number of malware variants, such as Shamoon, Duqu, Flame, and Gauss, which specifically target ICSs and have been used in various attacks [4]. Most notably, the BlackEnergy and CrashOverride attacks on Ukraine's power grid in 2015 and 2016 each caused power outages affecting more than 200,000 people [5]. These attacks were highly sophisticated and required substantial resources to develop and execute. However, with the growing number of smaller and less protected distributed energy resources (DERs), such as rooftop solar panels, the barrier to attack is lowered. The risks associated with lower attack barriers were exemplified by the attack on the Bowman Avenue Dam in New York in 2013 [4], where the attackers gained access to the SCADA system used to control local storm surges. Unlike other attacks on ICSs, the intrusion was not exceedingly sophisticated, and it is generally believed that the dam was targeted due to its minimal security [6,7]. The frequency of similar small-scale attacks on less protected cyber–physical systems is therefore expected to increase with the proliferation of DERs [8].

Cyberattack-detection methods for attacks on electric energy systems fall into three categories: network-based, data-driven, and model-based methods [9]:

Network-based methods for cyberattack detection aim to secure both internal and external communication channels [10]. External communications typically use encryption, network segmentation, and intrusion detection systems (IDSs) to complicate unauthorized access. Blockchain technology has been proposed for secure information sharing and patch management, including the distribution of blockchain clients, IDS updates, malware analysis results, and firmware changes [11]. While network-based detection methods can identify some attacks carried out via inverter communication channels, they are less effective against false data injection (FDI) attacks that manipulate sensor data either externally through physical-layer attacks such as Hall-sensor spoofing [12] or internally through malware embedded in the inverter control microcontroller. Such malware may be introduced through third-party vendor vulnerabilities [13] or supply chain attacks [14]. Given these vulnerabilities, it is impossible to ensure the system's cybersecurity by securing only the communication channels. Therefore, a defense-in-depth strategy that combines network-level detection with local inverter-side validation is essential [15].

Data-driven methods use machine learning (ML) models trained on historical data to detect FDI attacks and can be implemented at the local device level [9]. Reference [16] proposes a multilayer long short-term memory (MLSTM) network and evaluates its ability to detect and classify attacks using the voltage and current measurements from the PV array in a two-stage PV inverter. Reference [17] leverages various data-driven methods to evaluate micro-phasor measurement unit (μPMU) data at the point of common coupling (PCC) between an inverter and the grid to detect performance degradation caused by cyberattacks. Additionally, a hardware-in-the-loop (HIL) study compared the real-time operation of multiple data-driven methods for detecting and classifying attacks based on similar PCC measurements [18]. While these studies report very high accuracy, data-driven approaches lack physical interpretability and depend strongly on the quality and comprehensiveness of the training data, limiting their reliability against cyberattacks not represented in the training set.

Model-based detection methods use analytically derived system models to evaluate measurements. Common approaches include minimum mean square estimation for static systems [19], Luenberger observers for linear dynamics [20], and generalized Kalman filters for nonlinear systems [21]. These methods estimate system states and identify bad data when measurements deviate significantly from the model estimates [22]. While these methods were originally developed to detect low-quality measurements [23], they have been extended to cyberattack detection [19]. However, attackers with sufficient model

knowledge can construct stealthy attacks that evade such estimators [24]. Dynamic watermarking addresses this limitation by continuously injecting known excitations into the control signal and verifying their presence in the measured response [25,26]. Although [26] demonstrated consistent detection of both regular and stealthy attacks within 8 ms, the dynamic watermarking approach inevitably distorts the inverter output, negatively affecting its normal operation.

Motivated by the need for a non-disruptive detection method for FDI attacks, we propose an alternative watermarking approach for PV inverters that does not inject additional distortions. Our method first introduces two attack indicators that continuously validate inverter measurements against a state-space model to detect abnormal behavior, providing the benefits of model-based detection and enabling the detection of common FDI attacks, including noise injection and replay attacks. We then leverage the DC-link voltage fluctuations that naturally occur in PV inverters in response to irradiance variations [27] as a watermark, making it possible to reveal otherwise undetectable model-based attacks without additional distortions.

Specifically, the contributions of this paper are: (1) Unlike previous physical watermarking methods that introduce intentional distortions into control signals [25,26], our approach utilizes naturally occurring voltage fluctuations and therefore does not harm the inverter output. (2) We develop a HIL testbed for a two-stage grid-following PV inverter with irradiance-dependent DC-link voltage dynamics and use it to evaluate the proposed natural watermarking method under realistic DC-link voltage waveforms. Compared with our previous work, which modeled the DC-link voltage as an ideal voltage source with Gaussian noise [28,29], this testbed substantially improves waveform realism while retaining model performance. (3) We further validate the practical robustness of the detection architecture on a grid-forming hardware inverter platform with non-ideal sensing and real-time implementation constraints. This hardware study is used to assess implementation robustness and detector portability rather than to reproduce the full grid-following PV plant one for one. (4) The real-time implementation confirms the computational efficiency of our detection approach. The computational load of the model is evaluated against the baseline inverter control processes, confirming the feasibility for integration into existing inverter controllers without significant computational overhead.

The remainder of the paper is organized as follows. Section 2 describes the inverter system, the associated control loops, and the attacks on the system. Section 3 describes the proposed natural watermarking approach and how it has been modified for the HIL and hardware implementation. Section 4 shows the accuracy of the state-space estimator and the effectiveness of attack detection against each type of attack in the HIL environment. Section 5 evaluates the attack detection in a physical testbed. Finally, Section 6 summarizes the findings of this paper.

2. False Data Injection Attacks in PV Inverters

The architecture of the inverter system used in this paper is shown in Figure 1. From left to right, a PV array is connected to a boost converter, which feeds the DC-link capacitor of the inverter. The inverter converts this DC voltage to a three-phase AC output, which is connected to the grid through an LCL (inductor–capacitor-inductor) filter. Measurement signals from the DC-link voltage and the inverter outputs are processed by a digital signal processing (DSP) controller, which implements current control and DC-link voltage stabilization. FDI attacks are realized by embedding code on the DSP board, which intercepts and alters sensor signals before they enter the control loop. To detect these attacks, the DSP implements a natural watermarking model described in Section 3.

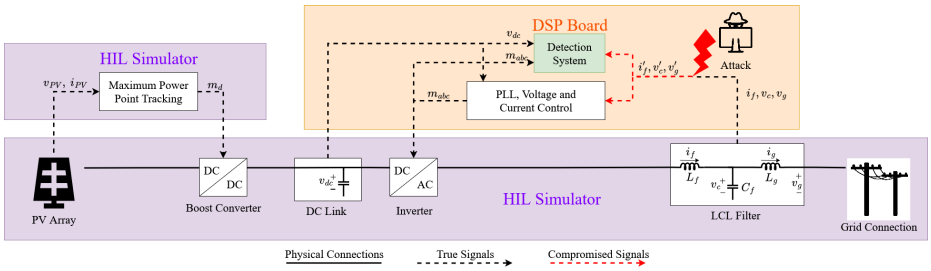


Figure 1. Block diagram of the hardware-in-the-loop (HIL) system testbed.

2.1. System Control

Maximum power point tracking (MPPT) for the PV array is achieved using a perturb-and-observe (P&O) algorithm to optimize power extraction from the panels [30]. As a result, the DC-link input current varies with solar irradiance. A phase-locked loop (PLL) ensures synchronization with the grid, and the AC signals used for current control are transformed into a synchronous direct-quadrature (dq) reference frame to simplify control implementation. In this frame, a proportional–integral (PI) controller regulates the DC-link voltage, v_{dc}, around its nominal value by generating the direct-axis current reference, $i^*_{f_d}$, which sets the inverter output current. The quadrature-axis current reference is set to zero, $i^*_{f_q} = 0$. PI current controllers then compute the modulation indices m_d and m_q from the current tracking errors, and these are transformed back to the modulation indices in the three-phase frame, i.e., m_a, m_b and m_c, to generate pulse-width modulation (PWM) signals for the inverter switches. Detailed equations and parameters are provided in Appendix A.

2.2. Threat Model

FDI attacks manipulate inverter behavior by modifying sensor measurements before they reach the inverter control loops. The controller therefore reacts to falsified measurements, causing it to deviate from normal operation and potentially damage the inverter or connected equipment. In this paper, the attacker is assumed to be able to observe and modify selected grid-side measurement signals before they are used by the inverter controller.

One possible attack vector is physical interference with the sensing hardware. Barua et al. [12] demonstrated that an electromagnet can be used to interfere with Hall-effect sensors used for voltage measurements. However, physical manipulation is less suitable for precise FDI attacks because the attacker has limited visibility into the recorded inverter measurements and is affected by uncontrolled variables such as sensor placement and electromagnetic shielding. Physical attacks are therefore limited to less advanced attacks such as the noise injection attack seen in Section 2.3.

More advanced attacks can be implemented through malicious code embedded in the controller or in the measurement-processing chain. Such malware may remain inactive until triggered by a timer, a control condition, or an external command and is referred to as a logic bomb [31]. Once triggered, the compromised sensing path modifies the measurements according to the attack strategy, and the distorted measurement propagates through the controller and affects the outputs. In the experimental implementation used in this paper, the attacks are programmed directly onto the DSP to ensure repeatability. This implementation emulates a compromised measurement path rather than unrestricted access to all controller resources. The attacker is therefore limited to manipulating the measurements and cannot rewrite the inverter control algorithm or directly change outputs. This is consistent with an attacker exploiting measurement calibration and recording functions rather than replacing the inverter firmware.

We assume that the attacker targets the grid-side measurements while the DC-link voltage measurement remains uncompromised. For physical attacks, this is motivated by

the fact that grid-side sensors are located near the grid connection point and are generally more accessible than the DC-link voltage sensor, which is located deeper inside the inverter. Digitally, the grid-side measurements describe the inverter's interaction with the external grid and are generally communicated to grid-support interfaces. These signals therefore have a larger attack surface and are more relevant to an attacker than internal DC-link measurements. Under this threat model, the DC-link voltage is considered a trusted internal signal for detecting inconsistencies caused by manipulated grid-side measurements.

2.3. Types of FDI Attacks

This paper specifically investigates three types of FDI attacks with increasing complexity and attacker knowledge requirements: noise injection, replay, and model-based attacks.

Noise-injection attacks degrade measurement quality by adding artificial noise to selected sensor signals. These attacks require the ability to alter the measurements, but they do not require system knowledge or previously recorded data. Although noise injection can quickly distort inverter operation, the resulting signals often differ significantly from normal behavior, making these attacks easier to detect.

Replay attacks replace real-time measurements with previously recorded data, breaking the correspondence between the physical inverter state and the feedback used by the controller. Such attacks require the ability to record and later replay measurements over a period of time, but they do not require any knowledge of the system model. Because replayed measurements resemble normal operation, replay attacks can be difficult to detect by monitoring only the compromised output signals [32].

Model-based attacks use a system model to generate realistic but false measurements. To execute a model-based attack, the attacker must therefore know the relevant measurements and control-loop outputs, as well as a sufficiently accurate model of the system dynamics. This enables the attack to remain stealthy while gradually driving the inverter toward harmful operating conditions, potentially causing accelerated component degradation or premature failure [24,33]. Due to their stealthy nature, model-based attacks are especially challenging to detect and are the primary motivation for the detection approach proposed in this paper.

2.4. DC-Link Voltage

Due to the transient behavior of the inverter controls, changes in the irradiance incident on the PV array trigger DC-link voltage fluctuations that can be used to reveal advanced FDI attacks. These dynamics are captured by the HIL model, and the voltage waveforms reflect what is observed in real systems. While the magnitude, duration, and waveform of these voltage deviations depend on the DC-link capacitance and controller gains, the transients are triggered and mainly defined by changes in irradiance. The timing and profile of these irradiance variations are further affected by cloud formation, which is governed by inherently stochastic atmospheric processes [34]. Additional site-specific effects, including panel degradation, soiling, and cell damage, further complicate the response [29]. As a result, without direct access to the sensor data, the corresponding DC-link voltage changes are exceedingly difficult to predict and can therefore help detect attacks by serving as a natural watermark. Because this watermark is already part of the normal operation, it is well-suited for detecting attacks that aim to cause gradual degradation.

3. Irradiance-Driven Natural Watermarking

The irradiance-driven natural watermarking approach requires five components: (1) a state-space model for predicting inverter behavior, (2) attack indicators for validating inverter measurements, (3) unpredictable DC-link voltage variations that act as

natural watermarks, (4) methods for mitigating measurement noise and model imperfections, and (5) a computationally efficient detection process that can run alongside the inverter controller.

3.1. State-Space Model

To simplify the inverter model and directly associate each measurement with its corresponding attack indicator, the state-space model is derived in the stationary *abc* reference frame. This avoids the balanced-measurement assumption implicit in the synchronous *dq* frame, which may not hold during an attack, and eliminates cross-coupling between phases, enabling independent phase analysis. The model is therefore derived for phase *a* and then replicated for phases *b* and *c*.

The phase *a* states are defined as the inductor currents and capacitor voltages of the LCL filter and stored in the state vector x_a. The system inputs, u_a, are defined as the inverter terminal voltage, v_{t_a}, and the grid voltage, v_{g_a}. The inverter-side output current, i_{f_a}, is chosen as the observed state, as it is already recorded and used in the current control loop.

$$x_a = \begin{bmatrix} i_{f_a} & i_{g_a} & v_{C_a} \end{bmatrix}^T \tag{1a}$$

$$u_a = \begin{bmatrix} v_{t_a} & v_{g_a} \end{bmatrix}^T \tag{1b}$$

$$y_a = \begin{bmatrix} i_{f_a} \end{bmatrix} \tag{1c}$$

While v_{g_a} is measured directly, v_{t_a} is calculated based on values from within the controller and the two-level inverter configuration [35]:

$$v_{t_a} = m_a \frac{v_{dc}}{2} \tag{2}$$

where m_a is the PWM modulation index for phase *a* and v_{dc} is the DC-link voltage. To derive the state equations, Kirchhoff's voltage and current laws are applied to the LCL filter while accounting for the series resistance of each component, where L_f and R_f correspond to the inverter-side inductor, L_g and R_g correspond to the grid-side inductor, and C_f and R_C correspond to the filter capacitor:

$$\dot{i}_{f_a} = -\frac{(R_f + R_C)}{L_f} i_{f_a} + \frac{R_C}{L_f} i_{g_a} - \frac{1}{L_f} v_{C_a} + \frac{1}{L_f} v_{t_a} \tag{3a}$$

$$\dot{i}_{g_a} = \frac{R_C}{L_g} i_{f_a} - \frac{(R_g + R_C)}{L_g} i_{g_a} + \frac{1}{L_g} v_{C_a} - \frac{1}{L_g} v_{g_a} \tag{3b}$$

$$\dot{v}_{C_a} = \frac{1}{C_f} i_{f_a} - \frac{1}{C_f} i_{g_a} \tag{3c}$$

The resulting A_a, B_a, and C_a matrices are thus defined as follows:

$$A_a = \begin{bmatrix} \frac{-(R_f+R_C)}{L_f} & \frac{R_C}{L_f} & \frac{-1}{L_f} \\ \frac{R_C}{L_g} & \frac{-(R_g+R_C)}{L_g} & \frac{1}{L_g} \\ \frac{1}{C_f} & \frac{-1}{C_f} & 0 \end{bmatrix} \tag{4a}$$

$$B_a = \begin{bmatrix} \frac{1}{L_f} & 0 \\ 0 & \frac{-1}{L_g} \\ 0 & 0 \end{bmatrix} \tag{4b}$$

$$C_a = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \tag{4c}$$

To enable digital implementation on the DSP, the Tustin approximation method is used to discretize the continuous-time matrices with the same sampling period as the control loop, $T_s = 100$ µs. This corresponds to the 10 kHz measurement and control rate used in the implementation. To reduce timing uncertainty, ADC sampling, state estimation, and control updates are synchronized with the inverter switching cycle. The PWM switching frequency is 20 kHz, while the measurement and control loops execute once every two switching periods. Because the ADC sampling and control update occur at fixed points in this cycle, sampling drift and variable data-collection delay are not included in the state-space model. Any remaining implementation delay is treated as part of the nominal prediction error and is accounted for through the baseline-removal and threshold-selection procedure described in Section 3.4. The resulting discrete-time state-space matrices (A_{d_a}, B_{d_a}, and C_{d_a}) enable the prediction of the state vector x_a and the output y_a at each discrete time step k:

$$x_a[k+1] = A_{d_a} x_a[k] + B_{d_a} u_a[k] \tag{5a}$$

$$y_a[k] = C_{d_a} x_a[k] \tag{5b}$$

The model states are initialized to zero during inverter startup and then evolve continuously with the measured inputs and modulation signals. Attack detection is evaluated after the estimator and moving-window baselines have settled, so startup transients do not affect the reported detection results. Component tolerances and discretization errors can introduce small prediction errors, but these errors are also included in the nominal baseline and threshold calibration described in Section 3.4. The resulting state-space model is therefore sufficiently accurate to support the proposed attack-detection method in both the HIL and hardware studies.

3.2. Attack Indicators

Two statistical attack-detection methods are employed to validate the output measurements based on the discrepancy between the measured output $z[k]$ and the predicted inverter outputs $y[k]$:

$$\Delta z[k] = |z[k] - y[k]| \tag{6}$$

During normal operation, $z[k]$ and $y[k]$ closely match each other, and $\Delta z[k]$ remains near zero. However, if an attacker interferes with the measurements, $z[k]$ will no longer match the predictions, resulting in larger values of $\Delta z[k]$. This is captured by the moving average test, (7), which calculates the average prediction error over a window of the n most recent measurements ending at the current time step l. An attack that increases the prediction error will therefore result in an increased value of (7), making the attack detectable.

$$\chi_1[l] = \frac{1}{n} \sum_{k=l-n+1}^{l} \Delta z[k] \tag{7}$$

Similarly, the moving variance test (8) quantifies the variability of $\Delta z[k]$ within the same window.

$$\chi_2[l] = \frac{1}{n} \sum_{k=l-n+1}^{l} (\Delta z[k] - \chi_1[l])^2 \tag{8}$$

Due to the squared difference in the calculation, (8) is more sensitive than (7) and is particularly effective at detecting noisy or rapidly changing attack patterns. Although (8) is more sensitive and will typically detect attacks before (7), combining both indicators is essential for the detection of some attacks. An attack that gradually introduces a DC bias into the measurement values would, for example, not affect the variance of the measurement

error and therefore be undetectable by (8). Similarly, an attack could be designed to hide within the system noise and evade detection by (7), but the higher sensitivity of (8) could still reveal such an attack. Thus, using both indicators provides redundancy, making it significantly more challenging to design an attack that simultaneously evades both indicators. However, an attacker with a state-space model of the system could potentially stay within both detection thresholds and would require a watermark to be identified.

3.3. Protected DC-Link Signal

A non-invasive watermark is constructed by using a state-space model to predict how DC-link voltage fluctuations propagate to the inverter output. Its effectiveness depends on the assumption that the attacker can manipulate output-side voltage and current measurements but cannot directly observe or alter the protected DC-link voltage measurement. In this work, the attacker can modify the AC-side sensor measurements used by the control loop and can generate false measurements using recorded data or a system model. However, the attacker is not assumed to have unrestricted access to all ADC channels, controller memory, or internally protected measurements. This assumption is consistent with an architecture in which the DC-link sensing path is isolated from the output-side measurement chain and protected independently. Under the threat model outlined in Section 2.2, the irradiance-driven variations in v_{dc} remain unavailable to the attacker and can therefore serve as a natural watermark. In a practical implementation, this assumption can be strengthened by applying additional protection to the DC-link voltage measurement, such as an isolated or encrypted signal path and restricted access to the corresponding DC-link voltage ADC channel.

An attacker could alternatively attempt to estimate the DC-link voltage based on AC-side measurements and the modulation indices. However, this would require an additional observer model, and the estimate would be complicated by switching behavior, nonlinear inverter dynamics, measurement noise, and uncertainty in the filter and controller parameters. This estimate would also be based on already observed input–output behavior and would therefore be delayed relative to the irradiance-driven DC-link transient. This limits its usefulness for generating falsified measurements that must remain consistent with the protected DC-link variation in real time. An attacker with direct access to the DC-link measurement, or with a sufficiently accurate real-time estimate of it, is therefore outside the threat model considered in this paper. Such a stronger attacker would require additional sensing-path, firmware, or hardware protections beyond the detection method considered here.

3.4. Noise Rejection and Detection Threshold

In a physical system, measurement noise and model imperfections inevitably cause a mismatch between the predicted and measured outputs even during nominal operation. As a result, the attack indicators (7) and (8) will return non-zero values during steady state. To reduce the masking effect of this nominal prediction error, the collection window n is chosen to yield a stable baseline, and the corresponding steady-state offsets are removed from both indicators.

Because the prediction error varies over the AC cycle, n is selected to span an integer number, i, of AC cycles:

$$n = i\frac{f_{\text{samp}}}{f_{\text{base}}}, \quad i \in \mathbb{Z} \tag{9}$$

With a sampling frequency of $f_{\text{samp}} = 10$ kHz and a grid frequency of $f_{\text{base}} = 60$ Hz, i is set to 3, resulting in a sliding-window length of $n = 500$ samples, corresponding to 50 ms. In this implementation, the attack indicators are therefore calculated over a window

spanning three AC cycles. The window length should therefore be treated as a tunable parameter where increasing n improves baseline stability and noise rejection, but also increases detection latency.

To remove the average prediction-error offset, precomputed steady-state baselines $\bar{\chi}_1$ and $\bar{\chi}_2$ are obtained under nominal conditions and subtracted from (7) and (8), resulting in the modified attack indicators:

$$\chi_1'[l] = \left| \left(\frac{1}{n} \sum_{k=l-n+1}^{l} \Delta z[k] \right) - \bar{\chi}_1 \right| \tag{10}$$

$$\chi_2'[l] = \left| \left(\frac{1}{n} \sum_{k=l-n+1}^{l} (\Delta z[k] - \chi_1[l])^2 \right) - \bar{\chi}_2 \right| \tag{11}$$

Even after baseline removal, χ_1' and χ_2' vary during nominal operation. To avoid false positive results and in accordance with standard practice for dynamic watermarking, the detection threshold for each detector is set to three times the maximum nominal value recorded during normal operation [26]. The exact threshold is implementation-dependent and is empirically determined from the maximum nominal indicator value recorded during calibration. This calibration includes steady-state operation at irradiance levels of 500 W/m^2, 800 W/m^2, and 1000 W/m^2, as well as transients between those levels. It therefore captures the combined effects of sensor noise, model mismatch, and irradiance-driven DC-link variation. In the implementations studied, no false positives were observed, and reliable detection was achieved for DC-link voltage deviations of approximately 5% to 10% from the reference value of 500 V. However, this range is specific to the tested systems and should not be interpreted as a universal requirement. The mismatch required to trigger detection is illustrated in Sections 4 and 5.

3.5. Computational Cost

Finally, a major challenge to implementing cybersecurity in ICSs is the limited computational resources [36]. If a security measure requires more resources than the device's standard operation, it may necessitate more advanced hardware, thereby increasing manufacturing costs and rendering implementation impractical. Therefore, the state-estimation and attack-detection tests must operate within the constraints of existing hardware. To assess this, the number of clock cycles required for the inverter controller to perform attack detection is recorded and compared with the clock cycles needed to execute the control tasks.

4. HIL Validation and Discussion

4.1. System Specifications

The system is implemented on a Typhoon HIL 506 real-time simulator (Typhoon HIL, Waltham, MA, USA) as shown in Figure 2. The simulation time step is 0.5 µs and the main system parameters are summarized in Table 1. The PV array is configured to deliver a nominal power of 2350 W, with an open-circuit voltage of 120 V and a short-circuit current of 25 A. The boost converter includes a 1 mH inductor feeding a 100 µF DC-link capacitor. The LCL filter consists of an inverter-side inductor $L_f = 2$ mH ($R_f = 1$ mΩ), a filter capacitor $C_f = 2$ µF ($R_C = 10$ mΩ), and a grid-side inductor $L_g = 2$ µH ($R_g = 4$ mΩ). The system interfaces with a 60 Hz three-phase grid rated at 120 V_{rms} line-to-line.

The control scheme described in Section 2.1 is implemented on a Texas Instruments F280049C DSP (Texas Instruments Inc., Dallas, TX, USA) and programmed using Code Composer Studio. The DSP uses a 100 MHz clock frequency, and both the inverter and boost controller use a 20 kHz switching frequency, while measurements and control loops

execute at 10 kHz. The DC voltage and output current control requires 5530 clock cycles (55.3 µs), and the complete detection procedure for each phase takes 1820 cycles (18.2 µs), with state estimation alone taking only 95 cycles (0.95 µs).

Table 1. HIL PV inverter system parameters.

Parameter	Symbol	Value
Real-time simulator	–	Typhoon HIL 506
Simulation time step	–	0.5 µs
PV array nominal power	P_{PV}	2350 W
PV open-circuit voltage	V_{OC}	120 V
PV short-circuit current	I_{SC}	25 A
Boost-converter inductance	L_{boost}	1 mH
DC-link capacitance	C_{dc}	100 µF
DC-link voltage reference	v^*_{dc}	500 V
Inverter-side filter inductance	L_f	2 mH
Inverter-side inductor resistance	R_f	1 mΩ
Filter capacitance	C_f	2 µF
Filter capacitor resistance	R_C	10 mΩ
Grid-side filter inductance	L_g	2 µH
Grid-side inductor resistance	R_g	4 mΩ
Grid frequency	f_{base}	60 Hz
Grid voltage	–	120 V_{rms} line-to-line
DSP	–	TI F280049C
DSP clock frequency	–	100 MHz
Switching frequency	f_{sw}	20 kHz
Control and sampling frequency	f_{samp}	10 kHz
Detection threshold DAC level	–	1.5 V

Cyberattacks are triggered through one of the DSP's input–output (I/O) ports using a signal generator. For real-time monitoring, attack indicators are output through the DSP's digital-to-analog converter (DAC) channels and recorded, along with inverter voltage and current waveforms. The gain of the DAC is tuned such that the attack detection threshold for each indicator corresponds to 1.5 V.

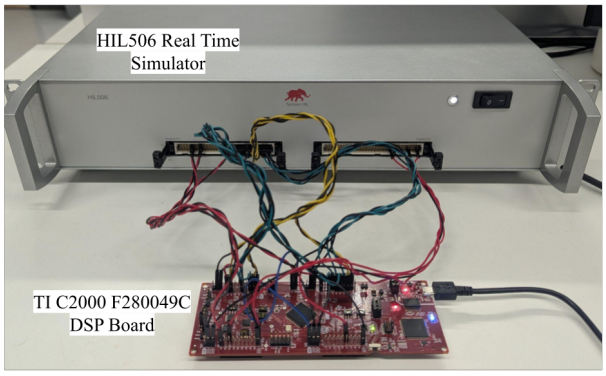


Figure 2. HIL testbed used for validation of natural watermarking for attack detection.

4.2. HIL Results

Although the signals from all three current measurements are attacked, our analysis focuses on the measurements from phase a, i_a. The procedure remains identical for all model states and phases and can be extended to an arbitrary number of measurements.

4.2.1. Model Quality

An accurate system model of the inverter outputs is essential for reliable attack detection. The modeled steady-state and transient performance is therefore evaluated by routing internal signals from the DSP board through its DAC channels and recording them with an oscilloscope. The measured signal (blue) and model prediction (orange) before and after a change in irradiance are plotted in Figure 3 and closely align, indicating strong agreement. Minor deviations arise from system noise and a slight phase shift introduced by the limited ADC sample rate.

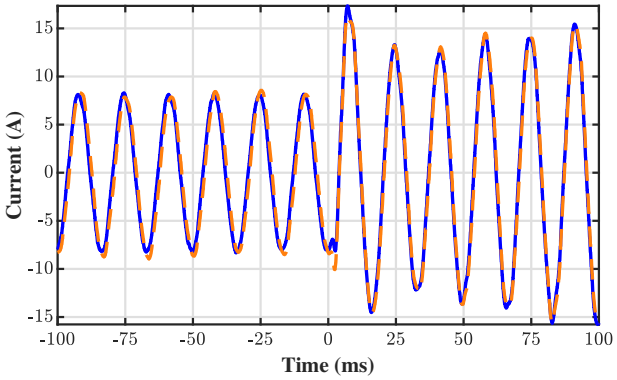
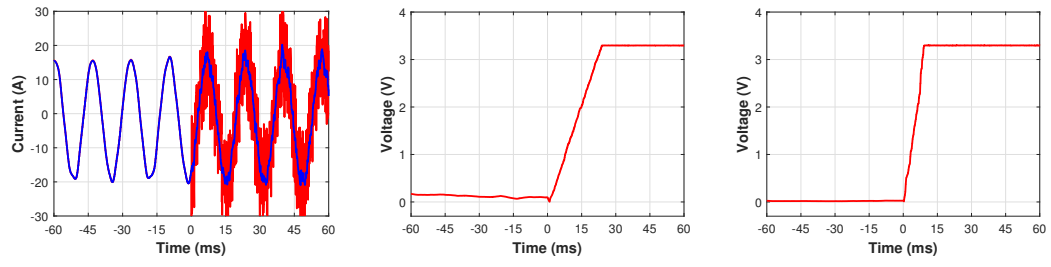


Figure 3. Measured signal (blue) and state-space model output (orange) of i_a before and after an irradiance change at $t = 0$.

4.2.2. Noise-Injection Attack on HIL

The impact of a noise-injection attack starting at $t = 0$ is illustrated in Figure 4a, which plots the true current of phase a (in blue) and the attacked measurement (in red). Once the attack is launched, the red curve shows how zero-mean Gaussian noise with a standard deviation equal to half the current amplitude is added to the true signal before it enters the control loop. After the attack is launched, the true output is also distorted, illustrating how the added noise propagates through the controller and distorts the inverter output. Figure 4b shows the moving average attack indicator, χ_1', while Figure 4c illustrates the moving variance indicator, χ_2'. Once the attack is initiated, both indicators increase rapidly before saturating at 3.3 V, which is the maximum output voltage of the DSP board. The moving variance test, χ_2', is most sensitive to noise and detects the attack within 5 ms.

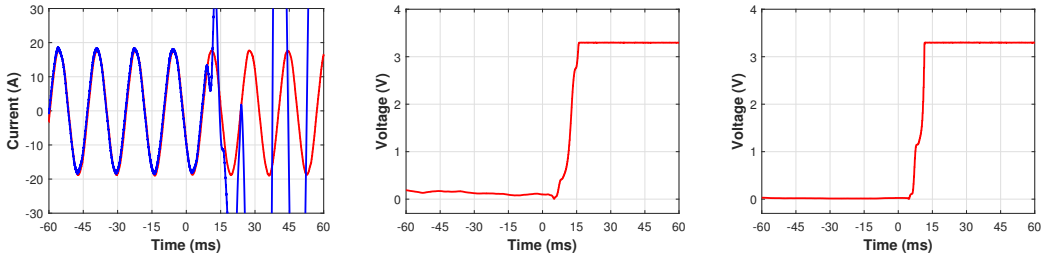


(**a**) (**b**) (**c**)

Figure 4. HIL-based detection of a noise-injection attack at $t = 0$ using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True i_a (blue) and measured i_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator.

4.2.3. Replay Attack on HIL

Figure 5a shows the true current of phase a (in blue) and the measurement under attack (in red) 60 ms before and after a replay attack is launched at $t = 0$. When the attack is launched, it breaks the closed-loop current control of the inverter. Although the controller continues to receive seemingly normal measurements, without the feedback path, the controller cannot correct any errors due to noise or varying operating conditions. As a result, the integral component of the PI controller grows indefinitely, rapidly destabilizing the inverter's output. Figure 5 shows how both attack indicators rise as the output current of the inverter starts to destabilize, rendering the attack detectable after approximately 10 ms.

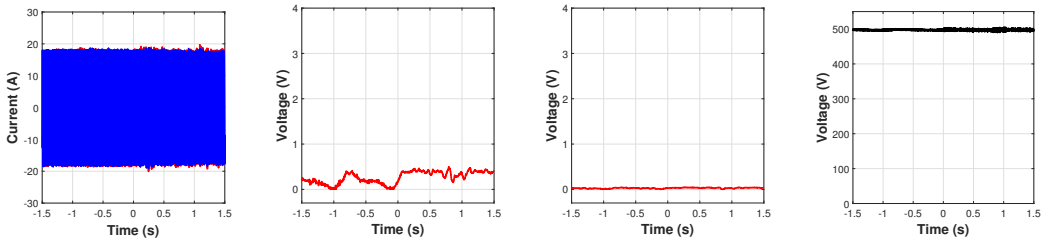


(**a**) (**b**) (**c**)

Figure 5. HIL-based detection of a replay attack at $t = 0$ using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True i_a (blue) and measured i_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator.

4.2.4. Model-Based Attack on HIL

During a model-based attack, the attacker uses their own state-space model of the inverter to generate realistic but falsified measurements. The attacked measurement therefore closely matches the state-space model used in the attack-detection process, making detection challenging. Consequently, during periods with no DC voltage fluctuations, the indicators cannot detect the attack. This behavior is demonstrated in Figure 6, which shows the DC-link voltage, output current, and both attack indicators over a three-second interval. The attack is launched at $t = 0$, but there are no detectable changes in χ_1' or χ_2'.



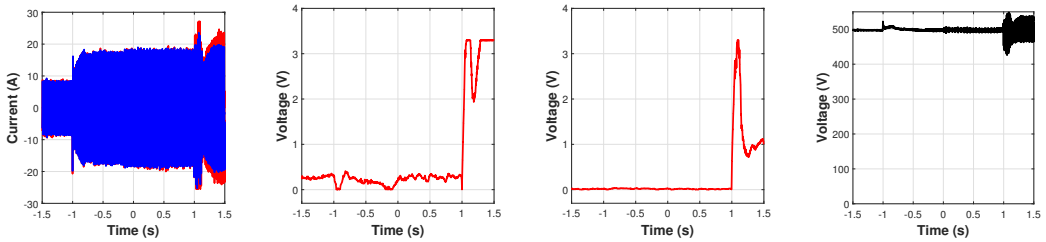
(**a**) (**b**) (**c**) (**d**)

Figure 6. HIL-based detection of a model-based attack at $t = 0$, with constant irradiance, using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True i_a (blue) and measured i_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator; (**d**) True v_{dc}.

Figure 7 shows the DC-link voltage, phase a output current, and corresponding attack indicators during a model-based attack scenario with variable irradiance. Here, the irradiance of the PV array changes from 500 W/m^2 to 1000 W/m^2 before the attack at $t = -0.75$ s, and then returns to 500 W/m^2 at $t = 1$ s after the attack is launched. Before the attack, the controller adjusts the output current to stabilize the DC-link voltage. However, without accurate knowledge of the DC voltage, the attacker cannot replicate the correct system response to the irradiance changes. This discrepancy results in instability of both the DC voltage and the output current, enabling detection of the attack. During the

post-attack irradiance change at $t = 1$ s, both indicators χ'_1 and χ'_2 increase significantly, clearly signaling the presence of the attack.

The transient events resulting from changes in irradiance can therefore reveal otherwise hidden attacks. While using these transients results in a longer detection time than dynamic watermarking, this is considered an acceptable trade-off when targeting stealthy attacks that aim to cause gradual component degradation.



(**a**) (**b**) (**c**) (**d**)

Figure 7. HIL-based detection of a model-based attack at $t = 0$, with variable irradiance, using the moving average-based (χ'_1) and moving variance-based (χ'_2) attack detectors. (**a**) True i_a (blue) and measured i_a (red); (**b**) χ'_1 attack indicator; (**c**) χ'_2 attack indicator; (**d**) True v_{dc}.

5. Hardware Validation and Discussion

Due to safety and practical implementation constraints, the hardware inverter platform differs from the grid-following PV system studied in the HIL environment. The purpose of the hardware test is therefore not to validate PV-side irradiance dynamics, but to evaluate whether the proposed detection architecture remains effective when applied to a physical inverter with non-ideal components.

Figure 8 shows the hardware testbed used to assess the practical implementation of the proposed detector. The PV array and boost stage are emulated by a programmable DC supply, the grid connection is replaced by a local load, and an LC filter replaces the LCL filter. However, the resulting platform preserves the key detection mechanism whereby DC-link variations that are unknown to the attacker propagate to the attacked measurements through the inverter dynamics.

In the hardware configuration, the inverter operates in grid-forming mode. Accordingly, the outer DC-link voltage loop is replaced by an AC voltage loop, the attacks are applied to output-voltage measurements, and the capacitor voltage is used as the observed state in the state-space model. The plots of the observed states are therefore in terms of capacitor voltage, but apart from these plant and control adaptations, the attack indicators, baseline-removal procedure, and residual-based detection logic remain unchanged.

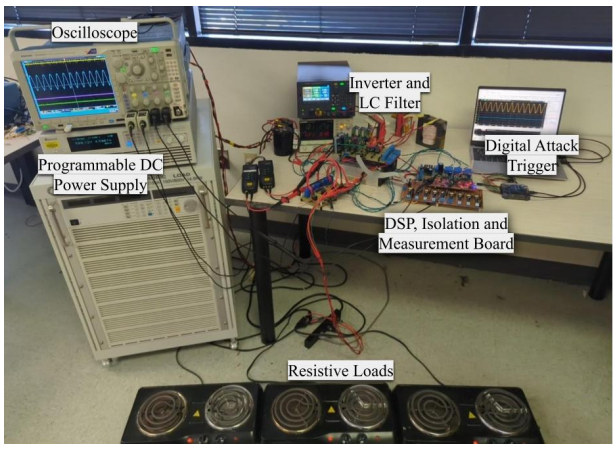


Figure 8. Hardware testbed used for validating natural watermarking for attack detection.

5.1. Hardware Specifications

A Chroma 62000H Series programmable power supply (Chroma ATE Inc., Irvine, CA, USA) delivers a nominal 500 V DC-link voltage and replicates voltage fluctuations observed in the HIL simulation. The main hardware-platform parameters are summarized in Table 2. The inverter converts this to a 60 Hz three-phase 120 V_{rms} AC output through an LC (inductor–capacitor) filter with nominal $L_f = 350$ µH ($R_f = 100$ mΩ) and nominal $C_f = 2$ µF ($R_C = 10$ mΩ), which is then supplied to a 2 kW resistive load. Voltage and current measurements at the inverter output and DC-link are obtained using LV25-P and LA 55-P transducers (LEM USA Inc., Milwaukee, WI, USA). To remove switching noise, the signals are processed through a passive first-order low-pass filter and an active second-order low-pass filter, then offset and scaled to remain within the 0 to 3.3 V input range of the DSP's ADC channels. These values are then sampled and fed to the control algorithm. Attacks are triggered by an external signal generator.

Table 2. Hardware inverter platform parameters.

Parameter	Symbol	Value
DC source	–	Chroma 62000H Series
Nominal DC-link voltage	v_{dc}	500 V
Inverter operating mode	–	Grid-forming
AC output frequency	f_{base}	60 Hz
AC output voltage	–	120 V_{rms} line-to-line
Filter topology	–	LC
Filter inductance	L_f	350 µH
Filter inductor resistance	R_f	100 mΩ
Filter capacitance	C_f	2 µF
Filter capacitor resistance	R_C	10 mΩ
Load type	–	Resistive
Load power	–	2 kW
Voltage transducer	–	LV25-P
Current transducer	–	LA 55-P
DSP	–	TI F280049C
DSP clock frequency	–	100 MHz
Switching frequency	f_{sw}	20 kHz
Control and sampling frequency	f_{samp}	10 kHz
Detection threshold DAC level	–	1.5 V

5.2. Hardware Results

5.2.1. Noise-Injection Attack on Hardware

Figure 9 shows the noise-injection attack. Once the attack starts at $t = 0$, Figure 9a shows a degradation of the output voltage, while the indicators in Figure 9b,c show a rapid increase in χ_1' and χ_2', making the attack detectable within approximately 5 ms. Despite the higher level of noise, this detection time remains similar to the HIL implementation.

5.2.2. Replay Attack on Hardware

Figure 10 shows the replay attack. Due to the slower voltage control loop, the inverter voltage in Figure 10a deviates more gradually than the output current seen in the HIL implementation. This renders the attack detectable after about 15 ms. Although detection is

slower compared to the noise-injection attack, detectability is proportional to the deviation from nominal operation, and the attack can therefore be identified before causing significant disruption to the system.

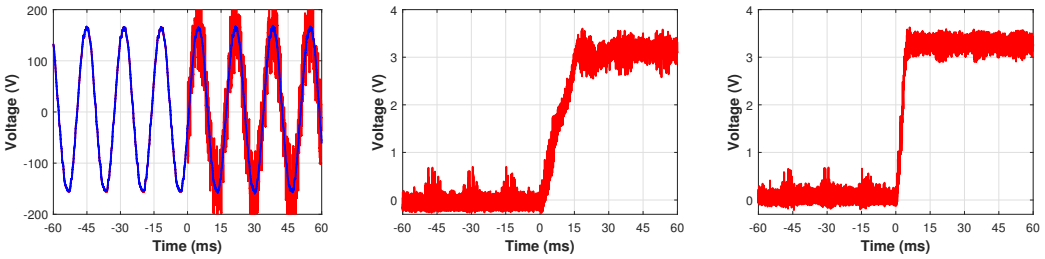


Figure 9. Hardware-based detection of a noise-injection attack at $t = 0$ using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True v_a (blue) and measured v_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator.

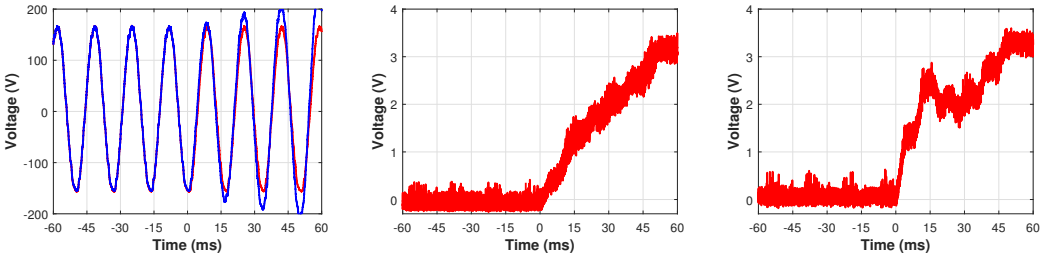


Figure 10. Hardware-based detection of a replay attack at $t = 0$ using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True v_a (blue) and measured v_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator.

5.2.3. Model-Based Attack on Hardware

Finally, the results of the model-based attacks, without and with DC-link voltage fluctuations, are shown in Figure 11 and Figure 12, respectively. Similar to the HIL implementation, the scenario without DC voltage changes shows no indication that the attack has been launched, and the attack remains undetectable. However, once DC-link voltage fluctuations are introduced, the attacker can no longer reproduce realistic measurements, and the inverter output diverges, as seen around the one-second mark in Figure 12a. This deviation from normal operation renders the attack detectable, as indicated by the rise in the χ_1' and χ_2' indicators in Figure 12b and Figure 12c, respectively.

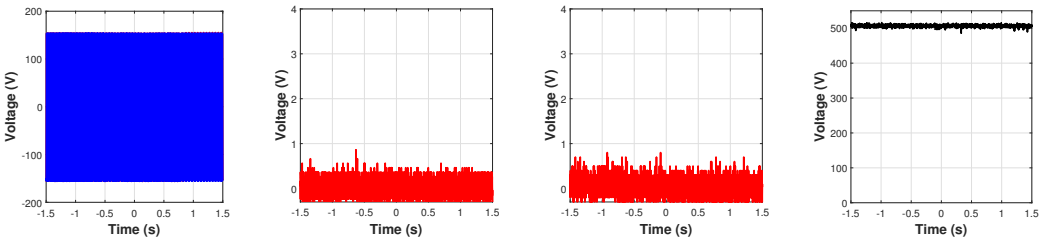


Figure 11. Hardware-based detection of a model-based attack at $t = 0$, with constant DC voltage, using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True v_a (blue) and measured v_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator; (**d**) True v_{dc}.

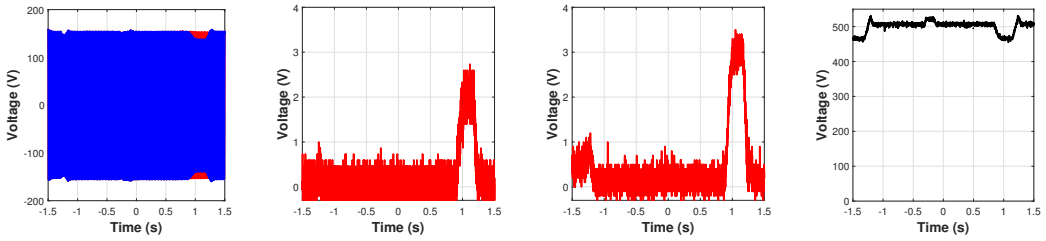


Figure 12. Hardware-based detection of a model-based attack at $t = 0$, with variable DC voltage, using the moving average-based (χ_1') and moving variance-based (χ_2') attack detectors. (**a**) True v_a (blue) and measured v_a (red); (**b**) χ_1' attack indicator; (**c**) χ_2' attack indicator; (**d**) True v_{dc}.

5.3. Hardware Discussion

The results of the hardware validation closely matched those observed in the HIL system, with a few notable differences. The most prominent change is the increased measurement noise, which is evident in the attack indicators. It should also be noted that the DC-link voltage changes observed during the model-based attack are more sharply defined in the hardware implementation. This difference arises due to the limited ramp rate and program complexity of the programmable power supply. The hardware implementation therefore does not fully replicate the dynamic interactions between the PV array, boost controller, and inverter. Instead, it serves as a physical validation platform for assessing the robustness of the state-space model and attack-detection algorithm, rather than as a one-to-one replication of the HIL testbed.

6. Conclusions

This paper proposes a natural-watermarking approach for local detection of FDI attacks in two-stage PV inverters. A HIL testbed with a grid-following inverter demonstrated that the two proposed attack indicators can quickly detect noise injection and replay attacks during steady-state conditions, while irradiance-driven DC-link fluctuations can function as a natural watermark and reveal model-based attacks that would otherwise remain undetectable. A modified hardware inverter platform further verified robustness to non-ideal sensing, component deviations, and real-time implementation constraints. The required computation was also shown to be compatible with standard inverter control tasks. These results should be interpreted within the proposed threat model and validation scope, noting that the natural watermark is most effective when irradiance changes produce DC-link voltage transients and that prolonged periods of constant irradiance may delay detection of stealthy model-based attacks. The method also relies on a protected DC-link voltage measurement, implementation-specific threshold tuning, and hardware validation that demonstrates implementation robustness rather than full reproduction of the HIL PV system. However, these results show that naturally occurring voltage fluctuations can serve as a non-invasive watermark for advanced attack detection without interfering with the normal inverter operation. Natural watermarking therefore provides a locally implementable detection method for revealing advanced FDI attacks when secure DC-link variations are present. Future work will expand the attack models to include partially informed and adaptive attackers, extend the approach to inverter-dominated microgrids, and develop mitigation strategies to reduce the impact of detected attacks.

Author Contributions: Conceptualization, L.B., I.B., T.H. and C.M.; methodology, L.B., I.B. and T.H.; software, L.B. and I.B.; validation and investigation, L.B. and N.V.K.; formal analysis, L.B., I.B., T.H. and C.M.; resources, T.H. and C.M.; writing—original draft preparation, L.B.; writing—review and

editing, I.B., T.H. and C.M.; supervision, N.V.K., T.H. and C.M.; funding acquisition, T.H. and C.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Science Foundation, grant number ECCS-2328205.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AC	Alternating current
ADC	Analog-to-digital converter
DAC	Digital-to-analog converter
DC	Direct current
DER	Distributed energy resource
DSP	Digital signal processor
FDI	False data injection
HIL	Hardware in the loop
ICS	Industrial control system
IDS	Intrusion detection system
LC	Inductor–capacitor
LCL	Inductor–capacitor–inductor
ML	Machine learning
MLSTM	Multilayer long short-term memory
MPPT	Maximum power point tracking
PCC	Point of common coupling
PI	Proportional–integral
P&O	Perturb and observe
PLL	Phase-locked loop
PV	Photovoltaic
PWM	Pulse-width modulation
SCADA	Supervisory control and data acquisition

Appendix A. Control System Specifications

This appendix summarizes the control algorithms used for the PV array, the HIL grid-tied inverter, and the hardware grid-forming inverter.

Appendix A.1. Grid-Forming Inverter

In the hardware implementation, the inverter operates in grid-forming mode with nominal angular frequency $\omega_0 = 2\pi \cdot 60$ rad/s. The AC output voltage is regulated by cascaded voltage and current control loops in the dq reference frame. The outer voltage loop generates the current references (i^*_{fd}, i^*_{fq}) and includes decoupling terms proportional to $\omega_0 C_f$ to reduce dq-axis coupling [37].

$$i^*_{f_d} = k_{pv}(v^*_{C_d} - v_{C_d}) + \frac{k_{iv}(v^*_{C_d} - v_{C_d})}{s} - \omega_0 C_f v_{C_q} \tag{A1}$$

$$i^*_{f_q} = k_{pv}(v^*_{C_q} - v_{C_q}) + \frac{k_{iv}(v^*_{C_q} - v_{C_q})}{s} + \omega_0 C_f v_{C_d} \tag{A2}$$

The AC voltage control loop is shown in Figure A1.

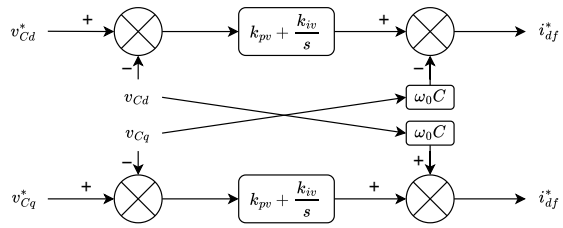


Figure A1. Inverter voltage control loop.

The current references, $i^*_{f_d}$ and $i^*_{f_q}$, are tracked by an inner current control loop. This control loop has a similar structure, but the decoupling terms are proportional to $\omega_0 L_f$ [37], where L_f is the inverter-side filter inductance:

$$v^*_d = k_{pi}(i^*_{f_d} - i_{f_d}) + \frac{k_{ii}(i^*_{f_d} - i_{f_d})}{s} - \omega_0 L_f i_{f_q} + v_{C_d} \tag{A3a}$$

$$v^*_q = k_{pi}(i^*_{f_q} - i_{f_q}) + \frac{k_{ii}(i^*_{f_q} - i_{f_q})}{s} + \omega_0 L_f i_{f_d} + v_{C_q} \tag{A3b}$$

The current control loop is illustrated in Figure A2.

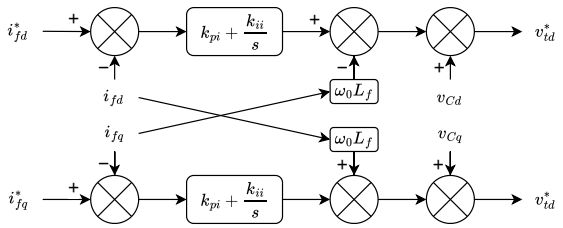


Figure A2. Inverter current control loop.

To compensate for DC-link voltage variations, feedforward scaling is used to generate the normalized modulation indices, m_d and m_q [35]:

$$m_d = v^*_d \frac{2}{v_{dc}} \tag{A4a}$$

$$m_q = v^*_q \frac{2}{v_{dc}} \tag{A4b}$$

Appendix A.2. Grid-Following PV Inverter

The HIL PV inverter uses a two-stage grid-following architecture consisting of an MPPT-controlled DC/DC converter and a grid-side inverter synchronized by a PLL. The inverter regulates the DC-link voltage by controlling the injected grid current.

Appendix A.2.1. PV Maximum Power Point Tracking

The MPPT controller for the PV array uses the perturb-and-observe (P&O) algorithm to determine the reference voltage v^*_{PV} [30]. At each time step k, the PV output voltage $v_{PV}[k]$ and current $i_{PV}[k]$ are measured to compute the power output:

$$P[k] = v_{PV}[k] \cdot i_{PV}[k] \tag{A5}$$

The change in power and voltage relative to the previous time step is then calculated as:

$$\Delta P[k] = P[k] - P[k-1] \tag{A6a}$$

$$\Delta v_{PV}[k] = v_{PV}[k] - v_{PV}[k-1] \tag{A6b}$$

The reference voltage is then updated as follows:

$$v_{PV}^{*}[k+1] = \begin{cases} v_{PV}^{*}[k] + \Delta v, \\ \quad \text{if } \Delta P[k] \cdot \Delta v_{PV}[k] > 0 \\ v_{PV}^{*}[k] - \Delta v, \\ \quad \text{if } \Delta P[k] \cdot \Delta v_{PV}[k] < 0 \end{cases} \tag{A7}$$

where Δv is the voltage perturbation step size.

The reference is tracked by a cascaded voltage-current loop that sets the boost-converter duty cycle, as shown in Figure A3:

$$i_{PV}^{*} = k_{p_{PV}}(v_{PV} - v_{PV}^{*}) + \frac{k_{i_{PV}}(v_{PV} - v_{PV}^{*})}{s} \tag{A8a}$$

$$m_{PV} = k'_{p_{PV}}(i_{PV}^{*} - i_{PV}) + \frac{k'_{i_{PV}}(i_{PV}^{*} - i_{PV})}{s} \tag{A8b}$$

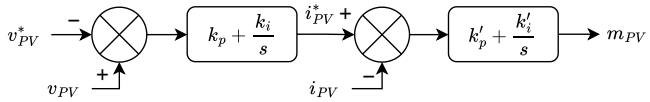


Figure A3. PV boost converter control loop.

Appendix A.2.2. Phase-Locked Loop

A synchronous-reference-frame PLL estimates the grid-voltage phase angle θ and angular frequency ω. The three-phase grid voltages $v_{g_{abc}}$ are transformed to the dq frame using the internal phase estimate, and the q-axis component v_{g_q} is regulated to zero by a PI controller. The estimated frequency is then integrated to obtain θ, with ω_0 included as a feedforward term.

$$\omega = k_{pPLL}(v_{g_q}) + \frac{k_{iPLL}(v_{g_q})}{s} + \omega_0 \tag{A9a}$$

$$\theta = \int \omega \, dt \tag{A9b}$$

The PLL structure is shown in Figure A4.

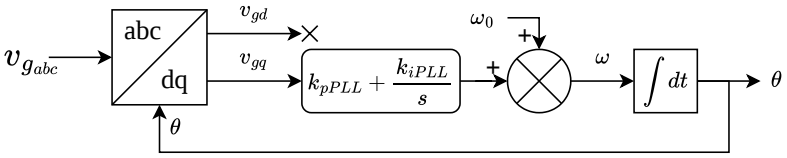


Figure A4. Three-phase PLL block diagram.

Appendix A.2.3. Grid-Tied Inverter

The grid-tied inverter uses a cascaded control structure where the outer DC-link voltage loop generates the current reference, and the inner current loop regulates the inverter-side current. The outer loop maintains the DC-link voltage near its nominal value $v_{dc}^{*} = 500$ V by generating $i_{f_d}^{*}$, while $i_{f_q}^{*}$ is set to zero:

$$i_{fd}^{*} = k_{pdc}(v_{dc}^{*} - v_{dc}) + \frac{k_{idc}(v_{dc}^{*} - v_{dc})}{s} \tag{A10a}$$

$$i_{fq}^{*} = 0 \tag{A10b}$$

The structure of this control loop is shown in Figure A5.

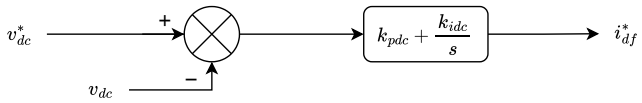


Figure A5. DC-link voltage control loop.

The inner current control loop is the same as for the grid-forming inverter and is described by (A3) and Figure A2.

Appendix A.2.4. Implementation and Controller Parameters

The controller gains and parameters used in the implementation are summarized in Table A1.

Table A1. Controller gains.

Parameter	Symbol	Value
Voltage loop proportional gain (grid-forming)	k_{pv}	2.51×10^{-3}
Voltage loop integral gain (grid-forming)	k_{iv}	314
Inverter current loop proportional gain	k_{pi}	2.2
Inverter current loop integral gain	k_{ii}	628
PV MPPT voltage perturbation	Δv	0.25
PV voltage loop proportional gain	$k_{p_{PV}}$	0.2
PV voltage loop integral gain	$k_{i_{PV}}$	4
PV current loop proportional gain	$k'_{p_{PV}}$	1×10^{-3}
PV current loop integral gain	$k'_{i_{PV}}$	2
Phase-locked loop proportional gain	k_{pPLL}	170
Phase-locked loop integral gain	k_{iPLL}	0.17
DC voltage loop proportional gain	k_{pdc}	5
DC voltage loop integral gain	k_{idc}	40

References

1. Rub-Rub, O.H.; Zare, A.; Zhang, Z.J.; Saeedifard, M.; Shadmand, M.; Mukherjee, S.; Hossain, R.R.; Adetola, V. Cybersecurity Challenges in Low-Inertia Power-Electronics-Dominated Grids. *IEEE Power Electron. Mag.* **2024**, *11*, 20–30. [CrossRef]
2. van Zalk, J.; Behrens, P. The spatial extent of renewable and non-renewable power generation: A review and meta-analysis of power densities and their application in the U.S. *Energy Policy* **2018**, *123*, 83–91. [CrossRef]
3. Kushner, D. The Real Story of Stuxnet. *IEEE Spectr.* **2013**, *50*, 48–53. [CrossRef]
4. Hemsley, K.E.; Fisher, E. *History of Industrial Control System Cyber Incidents*; Technical Report; Idaho National Laboratory (INL): Idaho Falls, ID, USA, 2018. [CrossRef]
5. Whitehead, D.E.; Owens, K.; Gammel, D.; Smith, J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *Proceedings of the 2017 70th Annual Conference for Protective Relay Engineers (CPRE)*; IEEE: New York, NY, USA, 2017; pp. 1–8. [CrossRef]
6. Prokupecz, S.; Kopan, T.; Moghe, S. Iranian Hackers Infiltrated New York-Area Dam Control System. 2015. Available online: https://www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam (accessed on 25 July 2025).
7. Nerger, J. Rye Brook Dam Caught in Computer Hacking Case. 2016. Available online: https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html (accessed on 25 July 2025).
8. U.S. Department of Energy. Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid Briefing. 2022. Available online: https://www.energy.gov/ceser/events/cybersecurity-considerations-distributed-energy-resources-us-electric-grid-briefing (accessed on 28 July 2025).
9. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A.; Kim, T.; Liu, J.; Chen, B.; Seo, G.S.; et al. A Review of Cyber–Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 4879–4901. [CrossRef]

10. Johnson, J.; Onunkwo, I.; Cordeiro, P.; Wright, B.J.; Jacobs, N.; Lai, C. Assessing DER network cybersecurity defences in a power-communication co-simulation environment. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*, 189–197. [CrossRef]
11. Ahn, B.; Bere, G.; Ahmad, S.; Choi, J.; Kim, T.; Park, S.W. Blockchain-Enabled Security Module for Transforming Conventional Inverters toward Firmware Security-Enhanced Smart Inverters. In *Proceedings of the 2021 IEEE Energy Conversion Congress and Exposition (ECCE), Virtual Conference, 10–14 October 2021*; IEEE: New York, NY, USA, 2021; pp. 1307–1312. [CrossRef]
12. Barua, A.; Faruque, M.A.A. Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*; USENIX Association: Berkeley, CA, USA, 2020; pp. 1273–1290.
13. SektorCERT. The Attack Against Danish Critical Infrastructure. 2023. Available online: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf (accessed on 11 August 2025).
14. FireEye. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. 2020. Available online: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (accessed on 28 July 2025).
15. Krause, T.; Ernst, R.; Klaer, B.; Hacker, I.; Henze, M. Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **2021**, *21*, 6225. [CrossRef] [PubMed]
16. Li, F.; Li, Q.; Zhang, J.; Kou, J.; Ye, J.; Song, W.; Mantooth, H.A. Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network. *IEEE Trans. Power Electron.* **2021**, *36*, 2495–2498. [CrossRef]
17. Li, Q.; Li, F.; Zhang, J.; Ye, J.; Song, W.; Mantooth, A. Data-driven Cyberattack Detection for Photovoltaic (PV) Systems through Analyzing Micro-PMU Data. In *Proceedings of the 2020 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA, 11–15 October 2020*; IEEE: New York, NY, USA, 2020; pp. 431–436. [CrossRef]
18. Zhang, J.; Guo, L.; Ye, J. Hardware-in-the-Loop Testbed for Cyber-Physical Security of Photovoltaic Farms. In *Proceedings of the 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Chicago, IL, USA, 28 June–1 July 2021*; IEEE: New York, NY, USA, 2021; pp. 1–7. [CrossRef]
19. Liu, Y.; Ning, P.; Reiter, M.K. False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [CrossRef]
20. Pasqualetti, F.; Dörfler, F.; Bullo, F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Proceedings of the 2011 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, FL, USA, 12–15 December 2011*; IEEE: New York, NY, USA, 2011; pp. 2195–2201. [CrossRef]
21. Meng, A.; Wang, H.; Aziz, S.; Peng, J.; Jiang, H. Kalman Filtering Based Interval State Estimation For Attack Detection. *Energy Procedia* **2019**, *158*, 6589–6594. [CrossRef]
22. Tan, S.; Guerrero, J.M.; Xie, P.; Han, R.; Vasquez, J.C. Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst. J.* **2020**, *14*, 5329–5339. [CrossRef]
23. Handschin, E.; Schweppe, F.; Kohlas, J.; Fiechter, A. Bad data analysis for power system state estimation. *IEEE Trans. Power Appar. Syst.* **1975**, *94*, 329–337. [CrossRef]
24. Sahoo, S.; Mishra, S.; Peng, J.C.H.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
25. Satchidanandan, B.; Kumar, P.R. Dynamic Watermarking: Active Defense of Networked Cyber–Physical Systems. *Proc. IEEE* **2017**, *105*, 219–240. [CrossRef]
26. Ibrahim, H.A.J.; Kim, J.; Ramos-Ruiz, J.A.; Ko, W.H.; Huang, T.; Enjeti, P.N.; Kumar, P.R.; Xie, L. Detection of Cyber Attacks in Grid-Tied PV Systems Using Dynamic Watermarking. *IEEE Trans. Ind. Appl.* **2024**, *60*, 819–827. [CrossRef]
27. Zhou, X.; Liu, Q.; Ma, Y.; Xie, B. DC-Link Voltage Research of Photovoltaic Grid-Connected Inverter Using Improved Active Disturbance Rejection Control. *IEEE Access* **2021**, *9*, 9884–9894. [CrossRef]
28. Balahewa, I.; Bjorndal, L.; Mi, C.; Huang, T. A Natural Watermarking Approach to Cyber Attack Detection for Power Electronics-Interfaced Renewables. In *Proceedings of the 2024 56th North American Power Symposium (NAPS), El Paso, TX, USA, 13–15 October 2024*; IEEE: New York, NY, USA, 2024; pp. 1–6. [CrossRef]
29. Balahewa, I.; Bjorndal, L.; Mi, C.; Huang, T. Cyber attack detection in renewable-rich IBR-dominated microgrids: A natural watermarking approach. *Electr. Power Syst. Res.* **2026**, *260*, 113148. [CrossRef]
30. Esram, T.; Chapman, P.L. Comparison of Photovoltaic Array Maximum Power Point Tracking Techniques. *IEEE Trans. Energy Convers.* **2007**, *22*, 439–449. [CrossRef]
31. Kabay, M.E. Crime, Use of Computers in. In *Encyclopedia of Information Systems*; Bidgoli, H., Ed.; Academic Press: Amsterdam, The Netherlands, 2003; Volume 1, pp. 345–363.
32. Mo, Y.; Sinopoli, B. Secure control against replay attacks. In *Proceedings of the 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 30 September–2 October 2009*; ACM: New York, NY, USA, 2009; pp. 911–918. [CrossRef]
33. Kim, B.; Ryu, K.; Back, J. A Generalized Hold Based Countermeasure Against Zero-Dynamics Attack With Application to DC-DC Converter. *IEEE Access* **2022**, *10*, 44923–44933. [CrossRef]

34. Knopf, D.A.; Alpert, P.A.; Zipori, A.; Reicher, N.; Rudich, Y. Stochastic nucleation processes and substrate abundance explain time-dependent freezing in supercooled droplets. *npj Clim. Atmos. Sci.* **2020**, *3*, 2. [CrossRef]
35. Yazdani, A.; Iravani, R. Control of Voltage-Sourced Converters. In *Voltage-Sourced Converters in Power Systems: Modeling, Control, and Applications*; Wiley-IEEE Press: Hoboken, NJ, USA, 2010; Chapter 5, pp. 115–126.
36. Tuyen, N.D.; Quan, N.S.; Linh, V.B.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [CrossRef]
37. Guo, W.; Mu, L. Control principles of micro-source inverters used in microgrid. *Prot. Control Mod. Power Syst.* **2016**, *1*, 5. [CrossRef]