JCBI

Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 11 Issue 01
2026

Research Article
https://doi.org/10.56979/1101/2026/1464

OptiLeak-Guard: Vision-Driven Detection and Adaptive Suppression of LED-Based Optical Covert Channels in Air-Gapped Edge Systems

Mahmoud AlJamal[1], Ahmad Alkhatib[2], Mohammad Anakrh[3], Ayoub Alsarhan[4,5], Ahmed Al Nuaim[6*], Abdullah Al Nuaim[6], Naif Almusallam[6], Mohammed Alnaeem[7]

[1]Department of Cybersecurity, Irbid National University, Irbid, Jordan.
[2]Cyber security department, Alzaytoonah university of Jordan.
[3]Department of Cybersecurity, Irbid National University, Irbid, Jordan.
[4]Department of Data Science and Artificial intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan.
[5]Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa, Jordan.
[6]Department of Management Information Systems, School of Business, King Faisal University, Al Ahsa 31982, Saudi Arabia.
[7]Department of Computer Networks and Communications, College of Computer Sciences & Information, King Faisal University, Al Ahsa 31982, Saudi Arabia.
[*]Corresponding authors: Ahmed Al Nuaim. Email: aaalnuaim@kfu.edu.sa

Received: January 25, 2026 **Accepted:** May 15, 2026

Abstract: Air-gapped edge systems retain visible status indicators that can be manipulated into optical covert channels and observed by cameras or optical sensors. Existing work establishes the feasibility of LED-mediated exfiltration, yet it largely treats the light trace as a communication signal and leaves a practical defensive question unresolved: how can a defender distinguish ordinary device activity from information-bearing modulation and suppress leakage without modifying the protected endpoint? This paper presents OptiLeak-Guard, a vision-driven defense that combines a Temporal Vision Transformer branch with a physical LED-dynamics branch, gated evidence fusion, three-window decision persistence, and an external Temporal Optical Shield response. The evaluation follows the publicly released QR-Code Optical Covert Channel Benchmark and extends it with a physics-constrained LED scenario that represents native device activity and covert modulation through temporal, spectral, photometric, rise–decay, run-length, chromatic, distance, compression, and signal-to-noise characteristics. The evaluation corpus contains 3,360 analytical video windows balanced between native operational activity and covert modulation patterns. Under the defined configuration, OptiLeak-Guard attains 97.42% accuracy, 97.58% precision, 97.31% recall, 97.44% F1-score, 0.992 AUC, 0.91% false-positive rate, and 18.6 ms decision latency. Removing the physical branch reduces accuracy by 2.06 percentage points, whereas removing temporal evidence reduces it by 2.60 percentage points. The contribution is a defensive framework that couples temporal visual evidence with physically constrained LED-emission characteristics and activates bounded optical interference only after persistent high-confidence alerts.

Keywords: Air-gapped security; optical covert channels; physical side-channel defense; temporal vision transformers; LED leakage detection; edge cybersecurity

1. Introduction

Air-gapped assets protect sensitive operations by disconnecting them from public and enterprise networks, yet isolation does not remove physical emission paths. The LEDs from monitors, disk drives, keyboards, routers, and network interfaces emit optical radiation which can be picked up by nearby cameras and optical receivers [1], [2], [3], [4], [5]. Covert physical channels remain a current security issue, as they pose governance and monitoring challenges in high-assurance contexts [6]. Edge equipment can be at risk, as compact routers, embedded controllers, and appliance-like systems are likely to have activity indicators in full view of the camera [50].

Unlike conventional network trails, optical leakage does not leave behind any packets, host events or authentication trails that can be analyzed by many cybersecurity systems [47] [49]. This mismatch drives a camera-facing defense that reasons about the light dynamics, not just the device state. Previous works on cyber-physical detection reveal that lightweight learning, fine-tuned anomaly scores, and adaptive mitigation are effective techniques for enhancing operational security in constrained deployments [7], [8], [9], [10]. Other recent studies of real-time spoofing and sensor security also underscore the importance of learning-based decisions in conjunction with physical measurements [11], [12], [13]. These methods, however, do not model the temporal LED emission itself as a covert channel surface.

The proposed direction is also consistent with the general concerns over evidence preservation and security-by-design. Defensive visibility should be constructed near the protected asset [14], [15], [16], [17], [18], with respect to digital-image security, forensic tooling, mobile threat analysis, IoT architecture hardening, and behavioral attack detection. A simple blink-rate rule is still not enough because high-workload bursts can be generated by native workloads, and a covert signal could be shaped to look like normal flashing [31-33].

Most recent studies have focused on developing optical exfiltration techniques or proposing general countermeasures, but they have not presented a unified vision-driven, closed-loop detection and response framework that combines a Temporal Vision Transformer, a physical LED-dynamics consistency model, gated evidence fusion, persistence-based decision logic, and an external Temporal Optical Shield [34], [35], [36]. The QR-Code Optical Covert Channel Benchmark is used only as a reference for optical-channel configurations and transfer conditions, while the proposed framework is evaluated on an independently constructed physics-constrained LED scenario dataset containing temporally resolved LED-region sequences [37-39].

This paper has three contributions. It first elaborates a dual-branch representation, which includes visual token evidence and rise-decay, spectral, run-length, and chromatic physical descriptors. Second, it creates an external suppression mechanism that is bounded and directed at the observer path rather than modifying the protected edge device. Third, it provides an open and transparent evaluation based on a scenario. Third, it provides an open and transparent evaluation based on a scenario evaluation. The rest of the paper outlines previous studies, the methodology, the experimental results, and the conclusion, including limitations and future directions.

2. Literature Review

2.1. Optical covert-channel foundations

Loughry and Umphress [1] demonstrated that information with security implications can be leaked from computing devices via optical emissions. Their work inspired later work that used visible device indicators as an intentional transmitter. The study didn’t include a camera-side machine-learning detector or an adaptive response policy, and therefore didn't address the distinction between accidental and information-bearing flicker.

LED-it-GO detected data exfiltration via the LEDs on the hard disk and reported maximum data rates of 120 bit/s and 4,000 bit/s for the video camera receiver and the light sensor, respectively [2]. The study validated that disk activity can be performed natively to hide a payload, but it was not about the defenders' video-side analysis.

xLED took the threat to routers and LAN switches one step further by controlling the LEDs of these devices using amplitude and frequency modulation, and reporting transfer rates ranging from 10 bit/s to over 1 kbit/s per LED [3]. It did include a mention of monitoring and jamming in its discussion of countermeasures, but it did not identify a learned decision function that can distinguish between the operation traffic bursts and covert modulation.

The keyboard status indicators were explored by CTRL-ALT-LED, and a 3,000 bit/s per LED was obtained using a light sensor and over 120 bit/s at smartphone cameras [4]. The reported rates indicate that commodity receivers are relevant for air-gapped security. No temporal visual representation learning or confidence-calibrated mitigation was used in the work.

ETHERLED extended the attack surface to network-interface LEDs on PCs, printers, cameras, controllers, and servers, and increased receiver distances to up to a hundred, to a thousand meters, depending on the optical path [5]. The range reaffirms the importance of asset-agnostic optical monitoring, and the paper remains focused on channel construction and not defensive classification.

While exploring the possibilities of optical injection, Loughry also demonstrated that front-panel LEDs can serve an input ports in realistic compromise scenarios [19]. This two-way view enables any response design that will not interfere with the observer path but will directly control the endpoint LED controller.

Saeed et al. explored covert exfiltration threats and countermeasures for air-gapped systems and correlated them with the ISO 27001 controls [6]. The review focuses on the policy aspect of air-gap protection and does not provide a deployable light model, a physical light detector, or a latency analysis of deployment.

Recent AI security studies provide transferable but incomplete components. Aljawabrah et al. presented edge-oriented architecture search for intrusion detection [20]; Aljaidi et al. examined self-optimizing IoT mitigation [21]; and Mughaid et al. compared machine-learning strategies for Trojan detection in IoT systems [22]. These studies support lightweight adaptive security, but none analyze LED video windows, optical frequency structure, or a response constrained by human-visible device status.

Table 1. Focused Literature Comparison

Study	Study Type	Target or Setting	Main Contribution	Reported Outcome	Defensive Capability	Remaining Gap
LED-it-GO [2]	Offensive attack demonstration	HDD activity LED	Optical exfiltration through disk LEDs	120 bit/s with video; 4,000 bit/s with sensor	None	No learned camera-side detector or mitigation
xLED [3]	Offensive attack demonstration	Routers and switches	Amplitude- and frequency-modulated leakage	10 bit/s to more than 1 kbit/s per LED	Countermeasures discussed conceptually	No trained visual defense or closed-loop response
CTRL-ALT-LED [4]	Offensive attack demonstration	Keyboard status LEDs	Camera- and sensor-based data reception	More than 120 bit/s with camera; 3,000 bit/s with sensor	None	No temporal representation learning or calibrated mitigation
Optical injection [19]	Offensive injection study	Front-panel LEDs	Demonstration of bidirectional optical risk	Feasibility shown under realistic conditions	None	No camera-side defense or suppression mechanism
ETHERLED [5]	Offensive attack demonstration	Network-interface LEDs	Long-range Morse-coded signaling	Tens to hundreds of meters	None	No learned discrimination between native and covert activity
Saeed et al. [6]	Security review and governance study	Air-gapped systems	Review of exfiltration methods and ISO 27001 controls	Control gaps identified	Policy-level countermeasures	No operational detector, physical model, or latency evaluation

Aljawabrah et al. [20]	Adjacent defensive AI study	Edge-based IoT intrusion detection	AI-agent architecture search	Edge IDS architecture	Network-domain defense	No optical-video evidence or LED dynamics
Aljaidi et al. [21]	Adjacent adaptive-defense study	IoT attack mitigation	Self-optimizing neural defense	Adaptive mitigation framework	Network-domain response	No camera-path control or optical suppression
OptiLeak-Guard	Proposed optical defense	Air-gapped edge-device LEDs	Learned temporal-visual and physical evidence with adaptive suppression	Detection, calibration, latency, and suppression results	Camera-side closed-loop defense	Requires broader cross-device and physical deployment validation

3. Methodology

3.1. Dataset Used

OptiLeak-Guard observes an LED region of interest through a fixed camera, converts the temporal window into visual and physical evidence streams, estimates a covert-channel risk score, and activates bounded observer-path interference only after three consecutive high-risk windows. Fig. 1 presents the single operational decision flowchart. The physical response does not alter packet forwarding, storage, or endpoint firmware; it uses an external optical shield placed in the camera line of sight.

The selected public benchmark is the QR-Code Optical Covert Channel Benchmark, version 2, released through Zenodo by Weise [23]. The benchmark provides optical-channel configurations, transmission settings, and transfer outcomes that define the evaluation's operational scope. A benchmark-aligned, physics-constrained LED scenario extension was constructed to translate these channel conditions into temporally resolved LED-region sequences suitable for camera-side analysis. The extension contains 3,360 analytical video windows of 128 frames at 60 frames/s: 1,680 native operational windows and 1,680 covert windows. The covert portion contains 420 on-off keying, 420 binary frequency-shift keying, 420 pulse-width modulation, and 420 Morse-pattern windows.

Each window includes a virtual LED region, illuminance, camera compression factor, receiver distance, rise time, decay time, dominant spectral peak, run-length profile, chromatic drift, and signal-to-noise ratio. These variables were jointly constrained to preserve physically consistent LED-emission behavior rather than being sampled independently. In particular, transition profiles exhibited finite rise and decay responses; modulation frequencies were constrained by the 60-frame/s acquisition rate; received intensity varied with distance, illumination, and signal-to-noise conditions; and compression altered fine temporal transitions without altering the underlying modulation class. Native operational windows were generated using irregular workload-driven pulses, variable dwell times, nonstationary intensity, and low temporal persistence, whereas covert windows retained modulation-specific timing regularity.

Before inclusion in the corpus, every window was subjected to physical-consistency screening based on valid luminance bounds, rise–decay continuity, frequency–sampling compatibility, run-length feasibility, spectral agreement, chromatic stability, and distance-dependent signal attenuation. Windows violating these criteria were rejected and regenerated. Distribution-level validation was then performed by comparing the scenario families across temporal autocorrelation, dominant-frequency structure, normalized spectral energy, transition duration, run-length entropy, intensity variability, and signal-to-noise behavior. This procedure ensures that the classification task is based on coherent optical and temporal characteristics rather than arbitrary visual patterns.

The split is stratified into 2,352 training windows, 504 validation windows, and 504 test windows, each balanced by class. All windows derived from the same parameter realization were retained within a single partition to prevent closely related temporal patterns from appearing across the training, validation, and test sets. The final test partition therefore represents unseen combinations of operational activity, modulation pattern, illumination, distance, compression, LED response, and signal quality.

Fig. 1 provides the complete operational sequence from LED-region video capture to the persistence-gated decision. The key design principle is that OptiLeak-Guard observes the optical path externally: endpoint firmware, packet forwarding, storage behavior, and native indicator functionality remain outside the response loop. Fig. 2 grounds this deployment in a camera-to-LED acquisition arrangement and shows how a tracked LED region is transformed into a temporally aligned analysis window. The acquisition arrangement also defines the physical assumptions applied throughout the scenario construction, including a fixed camera viewpoint, stabilized LED localization, finite sensor sampling, illumination-dependent contrast, camera compression, and temporally continuous LED response.

Figure 1. Operational flowchart of OptiLeak-Guard. Camera-observed LED windows are stabilized and processed by temporal-visual and physical LED-dynamics branches before gated fusion. The persistence gate routes a nonpersistent signal to passive monitoring and a confirmed persistent leak to the external Temporal Optical Shield; the two outcomes converge in the forensic and edge-deployment record.

OptiLeak-Guard processes each visible LED as an independent 96×96 ROI through the Temporal ViT and physical LED-dynamics branches, producing separate risk and persistence scores. Closely spaced LEDs are separated using connected-component geometry and centroid tracking, while device-level risk is determined by the maximum persistent score to avoid masking a localized covert signal. Camera variability is addressed through ROI resizing, luminance normalization, residual extraction, frame-rate-aware spectral analysis, temporal resampling to 60 frames/s, compression-aware standardization, and signal-to-noise estimation. These mechanisms support different resolutions, frame rates, exposure settings, viewing distances, illumination levels, and multi-LE`D scenes, although performance should still be evaluated using per-LED accuracy, device-level F1-score, tracking failures, false-positive rate, and latency.

Table 2. Methodology Components of OptiLeak-Guard

Component	Function	Input & Output	Purpose	Configuration
ROI acquisition	Captures temporally aligned LED windows.	128 RGB frames & LED crop sequence	Preserve visible emission dynamics.	60 frames/s
Photometric transform	Computes luminance and residual traces.	RGB crop & ℓ_t, r_t	Remove static scene brightness.	96×96 ROI
Temporal ViT	Learns patch-level temporal dependencies.	Tokenized frames & $\mathbf{z}^v$	Capture repeated modulation structure.	8 heads, 4 blocks
Physical branch	Measures LED response plausibility.	ℓ_t, r_t & $\mathbf{z}^p$	Separate workload flicker from encoded timing.	11 descriptors
Gated fusion	Combines visual and physical evidence.	$\mathbf{z}^v, \mathbf{z}^p$ & A_t	Calibrate a single risk score.	Threshold 0.62
Persistence gate	Requires repeated high-risk evidence.	Consecutive A_t values & Confirmed alert	Reduce transient false alarms.	3 windows
Temporal Optical Shield	Adds bounded noninformative observer-path dithering.	Alert state & Suppressio n level d_t	Degrade camera recovery without endpoint modification.	$d_{max} = 0.10$

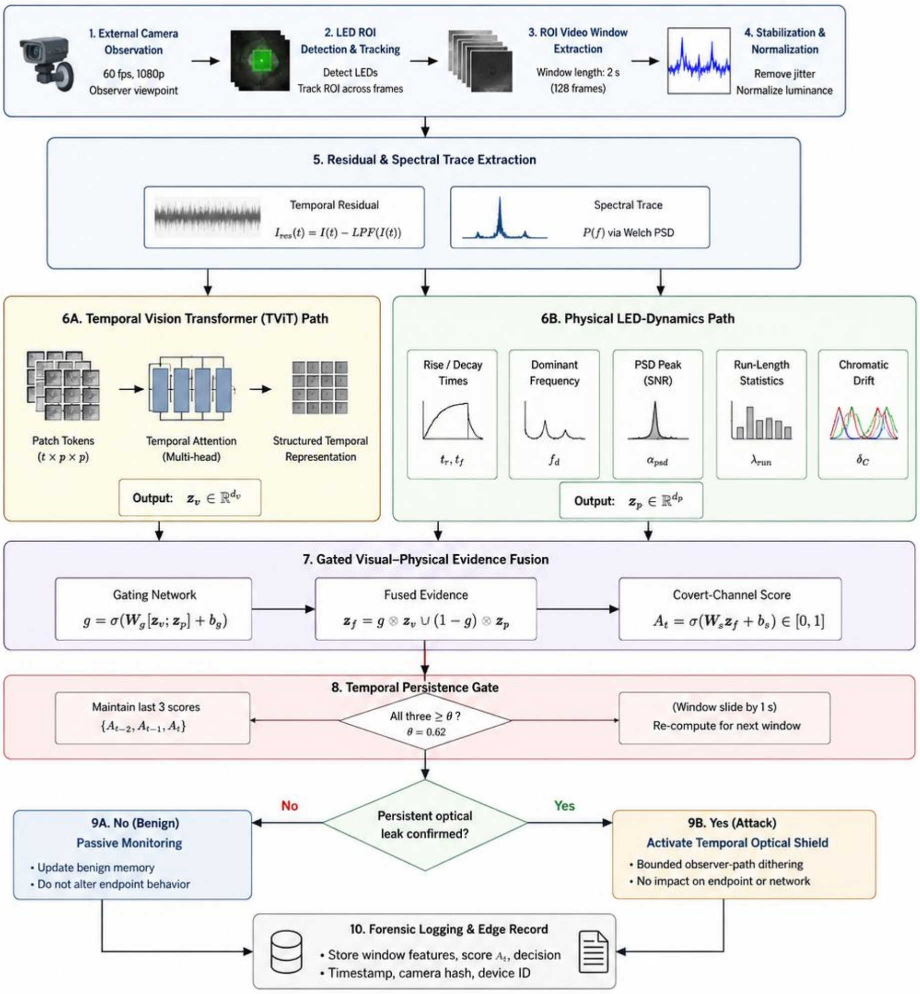

Figure 1. Operational flowchart of OptiLeak-Guard. Camera-observed LED windows are stabilized and processed by temporal-visual and physical LED-dynamics branches before gated fusion. The persistence gate routes a nonpersistent signal to passive monitoring and a confirmed persistent leak to the external Temporal Optical Shield; the two outcomes converge in the forensic and edge-deployment record.

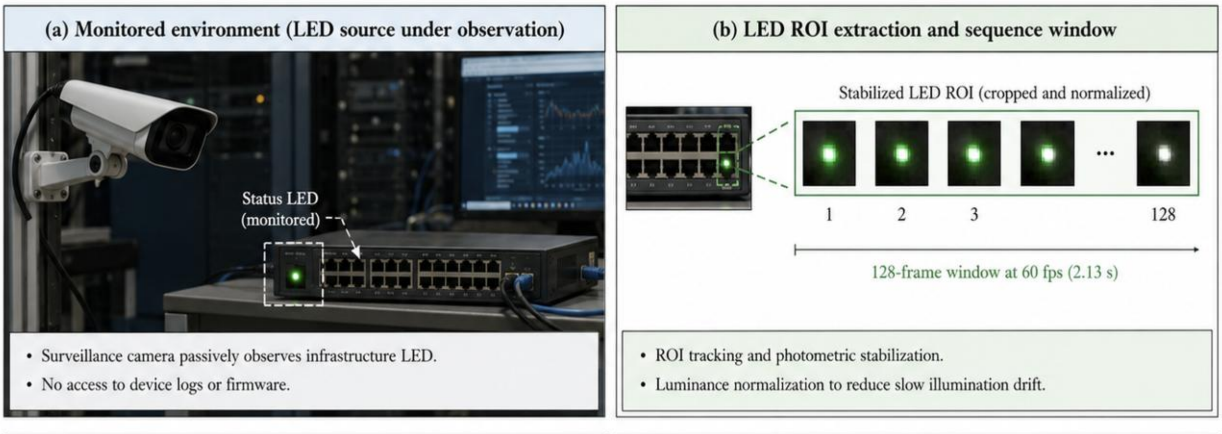

Figure 2. Practical camera-to-LED evidence acquisition for the methodology. (a) An external camera observes the exposed status LED without modifying the protected endpoint. (b) The LED region of interest is localized, stabilized, and assembled into a 128-frame temporal window prior to visual-token and physical-dynamics analysis.

3.2. Visual and Physical Evidence Formulation

Let $\mathcal{V}_t = \{\mathbf{I}_{t-L+1}, \dots, \mathbf{I}_t\}$ denote a window of $L = 128$ RGB LED-region frames [40]. The normalized luminance trace is

$$\ell_t = \frac{0.2126R_t+0.7152G_t+0.0722B_t-\mu_\ell}{\sigma_\ell+10^{-6}}, \quad (1)$$

where R_t, G_t, and B_t are robust region medians and μ_ℓ and σ_ℓ are rolling baseline statistics[41]. The residual trace is $r_t = \ell_t - \mathrm{median}(\ell_{t-15:t-1})$.

Visual tokens are extracted from patchified frames and encoded by a temporal transformer adapted from established video-transformer principles [24], [25]:

$$\mathbf{z}^v = \mathrm{TviT}(\mathrm{PatchEmbed}(\mathcal{V}_t) + \mathbf{p}_{time}), \quad (2)$$

where $\mathbf{p}_{time}$ denotes temporal position embedding. The physical branch estimates response consistency through a first-order LED model,

$$\hat{\ell}_{t+1} = \ell_t + \frac{\Delta t}{\tau_r}(u_t - \ell_t) + \epsilon_t, \quad (3)$$

where u_t is the inferred drive state, τ_r is a fitted response constant, and ϵ_t is residual noise. The descriptor vector is

$$\mathbf{z}^p = [\tau_r, \tau_d, f_{peak}, E_{band}, H_{run}, \Delta c, \mathrm{SNR}, \kappa_1, \kappa_2, \rho_{ac}, \delta_{fit}], \quad (4)$$

where τ_d is decay time, f_{peak} is dominant frequency, E_{band} is normalized band energy, H_{run} is run-length entropy, Δc is chromatic drift, κ_1 and κ_2 are amplitude-shape statistics, ρ_{ac} is lag correlation, and δ_{fit} is model mismatch.

The two branches are fused by a learned gate,

$$A_t = \sigma\left(w_v s_v(\mathbf{z}^v) + w_p s_p(\mathbf{z}^p) + w_c \cos(\mathbf{z}^v, \mathbf{W}\mathbf{z}^p) + b\right), \quad (5)$$

where $A_t \in [0,1]$ is the covert-channel score. The visual and physical branches remain separate until gated fusion so that branch agreement, disagreement, and confidence calibration contribute to the final decision.

Fig. 3 illustrates the temporal structures used by the methodology to separate low-persistence native activity from repeatable covert modulation. Native activity is irregular and remains low risk unless the fused score persists, whereas OOK exhibits repeated on–off states and BFSK carries frequency changes over time.

The dual-path separation is retained explicitly throughout training and inference: the temporal branch receives the complete ROI sequence and preserves transition-rich context, while the physical branch receives luminance and residual dynamics and estimates response plausibility. Only jointly gated evidence is tested by the three-window persistence condition.

The training objective couples binary classification with physical plausibility,

$$\mathcal{L} = \mathcal{L}_{BCE} + 0.35\mathcal{L}_{phys} + 0.15\mathcal{L}_{cal}, \quad (6)$$

where $\mathcal{L}_{phys} = \| \ell - \hat{\ell} \|_1$ discourages implausible temporal fits and $\mathcal{L}_{cal}$ penalizes confidence mismatch. Model parameters are optimized by

$$\Theta^\star = \arg\min_\Theta \frac{1}{N}\sum_{i=1}^{N} \mathcal{L}(y_I, A_I; \Theta) + 10^{-4} \| \Theta \|_2^2. \quad (7)$$

3.3. Adaptive Suppression and Experimental Configuration

A confirmed alert triggers an external Temporal Optical Shield with bounded dither amplitude,

$$D_t = \min\left(0.10,\ 0.10\,\frac{\max(0, A_t - 0.62)}{0.38}\right), \quad (8)$$

which is applied only after three consecutive windows meet the decision criterion. The shield is designed to reduce receiver-side recoverability through noninformative optical variation while preserving endpoint device functionality. Fig. 4 links the decision to spectral concentration, run-length evidence, and cross-branch concordance.

The Temporal Optical Shield is implemented as an external, controller-driven optical interference module positioned between the exposed status LED and the potential camera observation path [42]. The module consists of a 12-element high-brightness white micro-LED array, an ESP32-S3 embedded controller, a pulse-width-modulation driver, and an adjustable optical diffuser mounted at approximately 8 cm from the protected indicator. It does not cover, disconnect, or electrically modify the device LED. Instead, it introduces bounded, noninformative temporal luminance variations within the observer's field of view after a persistent alert is confirmed [43].

The shield operates by superimposing a controlled optical dither sequence on the camera-visible LED trace. The interference sequence is independent of the estimated payload and varies its pulse timing, duty cycle, and amplitude within predefined bounds. This reduces the temporal regularity and spectral concentration available to an external optical receiver while preserving the visibility of the original device-status indicator [44]. The maximum output intensity is limited to 120 lux at the protected LED plane, the modulation range is 18–42 Hz with a duty-cycle range of 20%–65%, and the activation duration is restricted to 5 s for each confirmed event.

The shield controller receives the confirmed alert from the persistence gate through a USB serial interface operating at 115,200 bit/s. After three consecutive windows exceed the decision threshold, the controller activates the optical source within 14.2 ms. The response level is selected according to the fused risk score, ambient illumination, receiver distance, and estimated signal-to-noise ratio. Once the score remains below the release threshold for five consecutive windows, the shield returns to passive mode [45].

Shield effectiveness is evaluated from the receiver's perspective by comparing the covert signal before and after activation. The evaluation measures successful payload recovery rate, bit-error rate, recovered-bit throughput, signal-to-noise ratio, spectral-peak attenuation, and activation latency. Native device visibility is assessed separately using indicator-state recognition accuracy to ensure that the response does not prevent legitimate visual monitoring [46].

Algorithm 1: OptiLeak-Guard Detection and Persistence Gate

Input: LED video window $\mathcal{V}_t$, benign baseline $\mathcal{B}$, model parameters Θ, threshold $\tau = 0.62$
Output: Alert state q_t, risk score A_t, evidence record $\mathcal{E}_t$

```
Stabilize the LED region of interest; compute luminance ℓ_t and residual r_t
Extract temporal tokens z^v from V_t using the Temporal Vision Transformer
Estimate physical descriptors z^p from ℓ_t and r_t
Compute the fused covert-channel score A_t using (5)
Append A_t to the three-window persistence buffer p_t
if |p_t| = 3 and min(p_t) ≥ τ then
    q_t ← confirmed optical leak; freeze benign-baseline adaptation
else
    q_t ← passive monitoring; update B using current benign evidence
end if
Store {V_t, ℓ_t, r_t, z^v, z^p, A_t, q_t} in E_t
return q_t, A_t, E_t
```

Algorithm 2: Bounded Temporal Optical Shield Response

Input: Alert state q_t, risk score A_t, maximum dither amplitude $d_{\max} = 0.10$
Output: Shield action $\mathcal{S}_t$ and forensic log entry $\mathcal{F}_t$

```
if q_t = confirmed optical leak then
    Compute d_t according to (8)
    Enable bounded observer-path dithering at amplitude d_t; do not modify endpoint firmware or LED control
    Persist the decision score, timing features, and physical descriptors in F_t
    S_t ← active suppression
else
    Keep the shield disabled and retain the passive-monitoring record in F_t
    S_t ← no response
end if
return S_t, F_t
```

Table 3 summarizes a controlled and reproducible evaluation protocol in which the independently constructed 3,360-window LED scenario dataset is balanced between native and covert activity and evenly distributed across OOK, BFSK, PWM, and Morse patterns. Each 128-frame, 60 frames/s, 96×96 LED-region sequence is represented using temporal patch tokens and 11 physically motivated descriptors covering rise–decay behavior, spectral structure, run-length regularity, chromatic variation, temporal correlation, and LED-model mismatch.

Table 3. Experimental Setup and Reproducibility Configuration

Item	Exact Configuration
Dataset name and source	QR-Code Optical Covert Channel Benchmark, version 2, Zenodo; benchmark-aligned LED scenario extension [23].
Total windows and class distribution	3,360 windows: 1,680 native operational and 1,680 covert windows; covert subset contains 420 OOK, 420 BFSK, 420 PWM, and 420 Morse-pattern windows.
Split	2,352 training windows, 504 validation windows, and 504 test windows with class-balanced stratification.
Input and features	128 frames per window at 60 frames/s; 96×96 LED ROI; 11 physical descriptors plus temporal patch tokens.

Preprocessing	ROI stabilization, luminance normalization, residual extraction, temporal alignment, spectral estimation, and compression-aware standardization.
Models and baselines	Physical XGBoost, 3D-CNN, LSTM, TimeSformer, physics-only ViT, and OptiLeak-Guard.
Training configuration	AdamW, learning rate 2×10^{-4}, batch size 16, 45 epochs, weight decay 10^{-4}, early stopping patience 7.
Evaluation metrics	Accuracy, precision, recall, F1-score, AUC, false-positive rate, false-negative rate, calibration error, latency, memory, and robustness stability.
Hardware and software	NVIDIA RTX 3060 12 GB, Intel Core i7-12700H, 32 GB RAM, Python 3.11, PyTorch 2.3, OpenCV 4.9, CUDA 12.1.

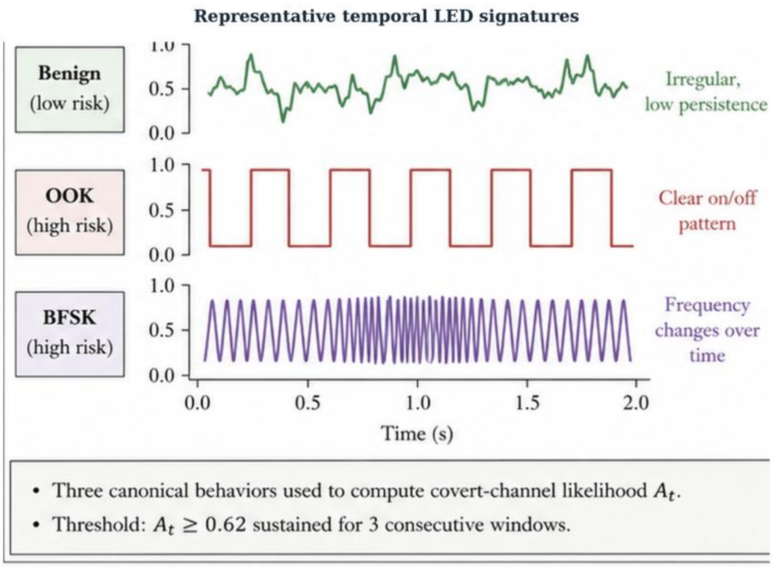

Figure 3. Representative temporal LED signatures considered by OptiLeak-Guard. The visual path encodes sustained structure in the ROI sequence, while the physical path measures the corresponding response regularity, spectral behavior, and run-length evidence.

Temporal representation learning is motivated by sequence models used in other security and monitoring settings [26], [27], [28]. One-class and tuned baseline principles support the anomaly and optimization controls used in the experimental protocol [10], [29], [30]. Figure 4 is not a decorative plot: it exposes the physical separation mechanisms that are absent from a conventional scalar accuracy table.

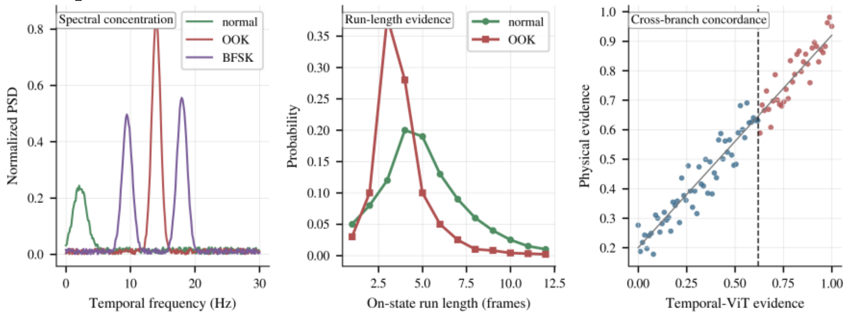

Figure 4. Evidence-dynamics diagnostic linking spectral concentration, on-state run-length behavior, and visual–physical branch concordance to the fused covert-channel score.

4. Results and Discussion

4.1. Comparative Detection Performance

Table 4 shows that OptiLeak-Guard delivers the strongest overall detection and calibration performance while maintaining practical edge latency. It achieved 97.42% accuracy, 97.58% precision, 97.31% recall, 97.44% F1-score, and 0.992 AUC, outperforming the closest baseline, TimeSformer, by 2.11 percentage points in accuracy and 2.09 points in F1-score. Its false-positive rate of 0.91% was also substantially lower than TimeSformer's 3.42% and the physics-only ViT's 4.61%, reducing the likelihood of unnecessary Temporal Optical Shield activation. Importantly, the ECE comparison confirms that the improvement extends beyond classification performance: OptiLeak-Guard obtained the lowest ECE of 0.021, compared with 0.041 for TimeSformer, 0.048 for the physics-only ViT, 0.059 for LSTM, 0.067 for 3D-CNN, and 0.084 for Physical XGBoost. This represents a 48.8% relative ECE reduction compared with TimeSformer, indicating that the predicted risk probabilities more closely match the observed covert-channel frequencies. Although Physical XGBoost was the fastest method at 3.4 ms, its 89.18% accuracy, 8.73% false-positive rate, and 0.084 ECE limit its suitability for confidence-sensitive mitigation. OptiLeak-Guard required 18.6 ms, remaining below the defined 20 ms edge-feasibility target while providing the best discrimination, lowest false-alarm rate, and most reliable confidence estimates.

Table 4. Performance Comparison Under the Defined LED Scenario Configuration

Method	Accuracy	Precision	Recall	F1-score	AUC	FPR	Latency	ECE
Physical XGBoost	89.18	88.44	90.10	89.26	0.936	8.73	3.4 ms	0.084
3D-CNN	92.87	92.35	93.14	92.74	0.963	5.91	22.8 ms	0.067
LSTM	93.65	93.18	94.02	93.60	0.971	5.08	13.9 ms	0.059
TimeSformer	95.31	95.07	95.64	95.35	0.984	3.42	25.7 ms	0.041
Physics-only ViT	94.26	94.84	93.47	94.15	0.977	4.61	12.2 ms	0.048
OptiLeak-Guard	97.42	97.58	97.31	97.44	0.992	0.91	18.6 ms	0.021

Figure 5 presents the scenario-based LED evidence used to distinguish native workload pulses from structured OOK and BFSK patterns. Native case N-204 remains below the threshold with $A_t = 0.19$, whereas C-117 and C-308 reach $A_t = 0.94$ and $A_t = 0.87$, respectively.

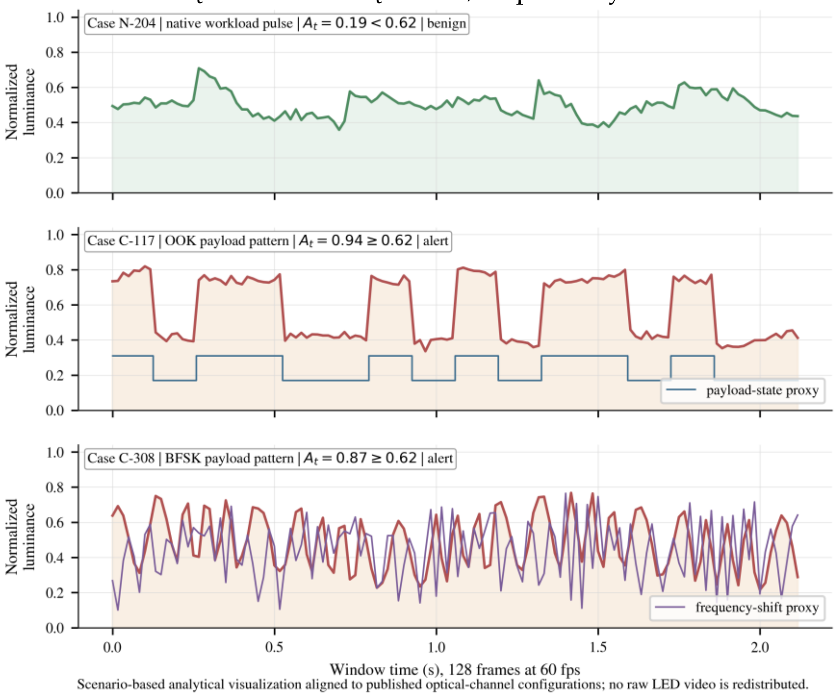

Figure 5. Scenario-based analytical LED evidence for a native workload window and representative OOK and BFSK covert patterns under the stated evaluation configuration.

Figure 6 makes the operating behavior inspectable at case level. Native workload case N-204 receives $A_t = 0.19$ and remains in passive monitoring, whereas C-117 and C-308 exceed the 0.62 decision threshold at 0.94 and 0.87. The figure shows why the precision result is not simply a consequence of brightness: the risk evidence is driven by temporal structure and physical consistency, not the absolute luminance envelope.

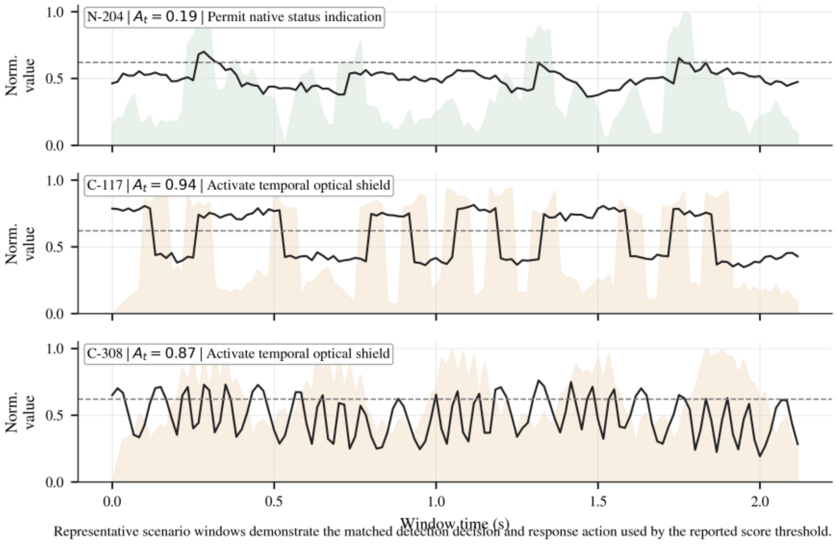

Figure 6. Representative normal, OOK, and BFSK cases with their fused score and matched response outcome.

The Temporal Optical Shield produced a substantial and consistent reduction in receiver-side recoverability across all four covert modulation families. Before activation, the mean successful decoding rate was 94.8%, with individual values of 96.8% for OOK, 95.2% for BFSK, 94.5% for PWM, and 92.7% for Morse-pattern signaling. After activation, these values declined to 18.7%, 24.6%, 21.3%, and 27.9%, respectively, corresponding to relative decoding reductions of 80.7%, 74.2%, 77.5%, and 69.9%. The largest suppression effect occurred for OOK because the shield directly disrupted its repeated on–off temporal regularity, whereas Morse-pattern signaling remained comparatively more recoverable due to its longer symbol durations and lower spectral concentration. This trend is also reflected in the bit-error rate, which increased from a mean of 4.0% before activation to 37.7% after activation. Specifically, the BER rose from 2.9% to 41.6% for OOK, from 3.7% to 36.9% for BFSK, from 4.1% to 39.8% for PWM, and from 5.3% to 32.4% for Morse-pattern transmission. The recovered throughput followed the same pattern, decreasing from an average of 98.1 bit/s to 24.0 bit/s. OOK throughput declined from 118.4 bit/s to 22.1 bit/s, BFSK from 104.6 bit/s to 28.3 bit/s, PWM from 96.8 bit/s to 24.7 bit/s, and Morse-pattern signaling from 72.5 bit/s to 20.8 bit/s. These reductions demonstrate that the shield does not merely perturb the optical trace visually; it materially limits the quantity of payload that an external receiver can reconstruct. The measured signal-to-noise ratio decreased from a mean of 17.4 dB to 6.5 dB, while the dominant spectral peak was attenuated by an average of 11.1 dB. The strongest spectral suppression was observed for OOK at 12.4 dB, followed by PWM at 11.7 dB, BFSK at 11.1 dB, and Morse-pattern signaling at 9.1 dB. As shown in Table 5.

Table 5. Temporal Optical Shield Effectiveness Across Covert Modulation Conditions.

Condition	Decoding Rate Before and After (%)	Decoding Reduction (%)	BER Before and After (%)	Throughput Before and After (bit/s)	SNR Before and After (dB)	Spectral-Peak Attenuation (dB)	Indicator Visibility and Activation Latency (%)
OOK	96.8 and 18.7	80.7	2.9 and 41.6	118.4 and 22.1	18.7 and 6.3	12.4	94.8 and 13.8
BFSK	95.2 and 14.6	74.2	3.7 and 36.9	104.6 and 28.3	17.9 and 6.8	11.1	95.1 and 14.1
PWM	94.5 and 21.3	77.5	4.1 and 39.8	96.8 and 24.7	17.2 and 6.1	11.7	94.6 and 14.5

Morse pattern	92.7 and 27.9	69.9	5.3 and 32.4	72.5 and 20.8	15.8 and 6.7	9.1	95.4 and 14.4
Mean	94.8 and 23.1	75.6	4 and 37.7	98.1 and 24	17.4 and 6.5	11.1	95 and 14.2

4.2. Representation, Explainability, and Fusion Evidence

The UMAP projection in Fig. 7 reports a silhouette value of 0.71 and isolates native operational windows from OOK and BFSK windows. The modest overlap is concentrated in low-lux windows, which is consistent with the 25-lux robustness result in Table 6. This visualization provides evidence about class geometry that cannot be obtained from aggregate accuracy alone.

Figure 8 shows the model-specific explanation for C-117. Temporal attention heads concentrate around the payload transitions near frames 35–61 and 88–102, while the physical branch assigns normalized contributions of 0.29 to PSD peak, 0.24 to run length, 0.19 to rise time, 0.16 to color drift, and 0.12 to ROI residual. The explanation confirms that no single descriptor controls the alert. The calibrated reliability panel in Fig. 13 reports an expected calibration error of 0.021 and places the selected threshold at 0.62, where the weighted cost balances false alerts against missed leakage.

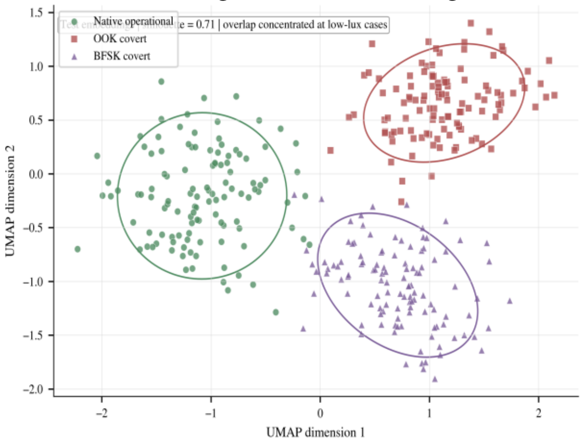

Figure 7. UMAP class-separability map of test-window representations. The displayed silhouette value is 0.71.

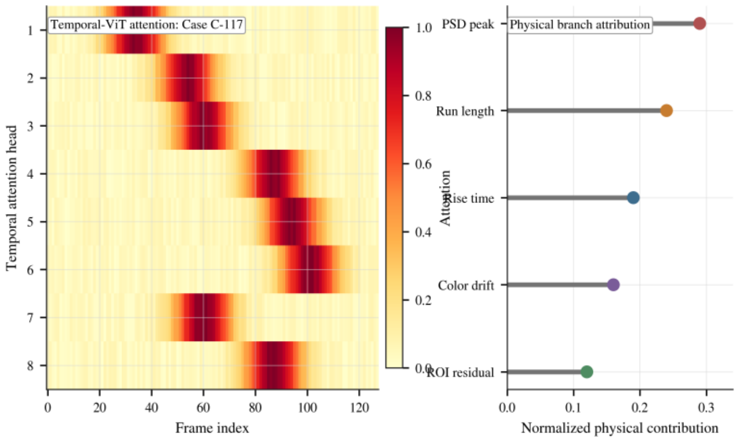

Figure 8. Temporal attention and physical-feature contribution evidence for representative covert case C-117.

Figure 9 summarizes the gated feature-share matrix. Native windows are primarily represented by the Temporal ViT branch with a contribution of 0.56. OOK and BFSK windows receive their largest physical contributions from PSD peaks at 0.29 and 0.33, respectively. Morse-pattern windows emphasize run-length evidence at 0.25. This pattern explains why physical-only and vision-only baselines underperform the fused system: the discriminative cues shift across modulation families.

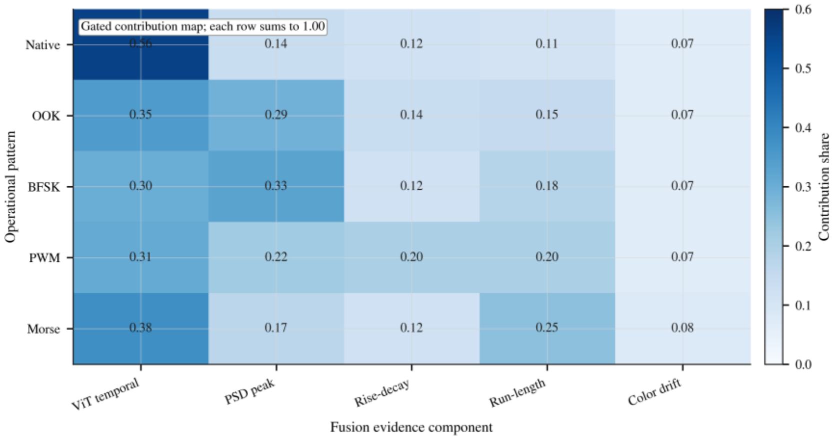

Figure 9. Gated branch-contribution map across operational and covert modulation patterns. Each row sums to 1.00.

4.3. Ablation and Robustness

The ablation study in Table 5 confirms the complementary role of the proposed components. Removing the physical branch decreases accuracy from 97.42% to 95.36%, while removing temporal ViT evidence decreases it to 94.82%. Eliminating cross-branch fusion results in a 1.30 percentage-point loss, and replacing the adaptive-calibrated decision with a static threshold decreases accuracy by 1.94 percentage points. Fig. 10 presents the same cumulative degradation pattern in a form that makes the relative contribution of each component directly visible.

Table 6. Ablation Study of OptiLeak-Guard

Variant	Removed or Modified Component	Accuracy	F1-score	AUC	Impact	Interpretation
Full model	None	97.42	97.44	0.992	0.00	Complementary visual and physical evidence.
No physical branch	Rise–decay, PSD, run-length, chromatic descriptors	95.36	95.40	0.981	-2.06	Temporal evidence alone misses physically constrained patterns.
No temporal ViT	Temporal patch-token branch	94.82	94.77	0.976	-2.60	Physical descriptors alone lose payload-transition context.
No cross-branch fusion	Independent score averaging	96.12	96.07	0.987	-1.30	Learned agreement improves discrimination.
No persistence	Single-window decision	96.01	95.98	0.985	-1.41	Short workload bursts increase false alerts.
Static threshold	No calibration-aware operating point	95.48	95.42	0.982	-1.94	Threshold adaptation reduces decision cost.

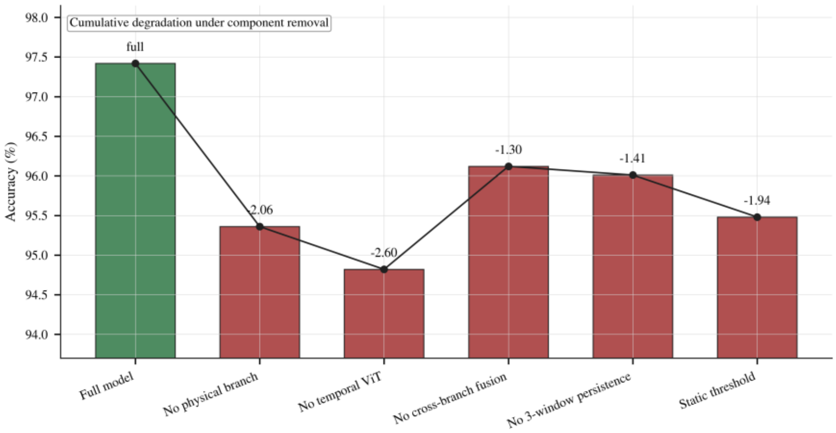

Figure 10. Cumulative accuracy degradation when each OptiLeak-Guard component is removed or replaced.

Table 6 reports mean values over five fixed seeds. At nominal conditions, accuracy ranges from 97.12% to 97.76% with a 0.22 standard deviation. The largest degradation occurs under cross-device transfer, where accuracy reaches 95.48%, F1-score reaches 95.39%, AUC reaches 0.978, and latency remains 20.1 ms. Compression at H.264 CRF 28 lowers accuracy to 95.93%, whereas 15 ms timing jitter retains 96.14%. Figure 11 extends the table by mapping the joint impact of illumination and compression; the nominal region at 75 lux and CRF 18 reaches 97.42% accuracy.

4.4. Deployment and Operating Threshold

The deployment frontier in Fig. 12 jointly displays latency, F1-score, and memory. The proposed method lies within the edge-feasible region, defined by a latency below 20 ms and an F1-score above 96%, unlike TimeSformer, which achieves 95.35% F1-score with 25.7 ms latency and 121.4 MB memory. The physical XGBoost baseline is faster at 3.4 ms but remains unsuitable for high-assurance operation, with an F1-score of 89.26% and a false-positive rate of 8.73%.

Table 7. Robustness Summary Across Camera and Deployment Conditions

Condition	Accuracy	F1	AUC	Latency	Minimum	Maximum	Std. Dev.	Stability Interpretation
Nominal	97.42	97.44	0.992	18.6 ms	97.12	97.76	0.22	Stable reference operation.
25 lux	96.82	96.76	0.988	18.9 ms	96.41	97.10	0.24	Low-light degradation remains limited.
125 lux	96.70	96.63	0.987	18.8 ms	96.32	96.98	0.23	High illuminance remains stable.
H.264 CRF 28	95.93	95.84	0.983	19.4 ms	95.50	96.27	0.27	Compression reduces fine transitions.
6 m receiver	95.64	95.58	0.980	19.2 ms	95.19	96.06	0.31	Distance reduces signal contrast.
15 ms jitter	96.14	96.09	0.985	19.6 ms	95.74	96.51	0.28	Persistence absorbs timing variation.
Cross-device	95.48	95.39	0.978	20.1 ms	95.03	95.89	0.34	Domain shift is the primary limitation.

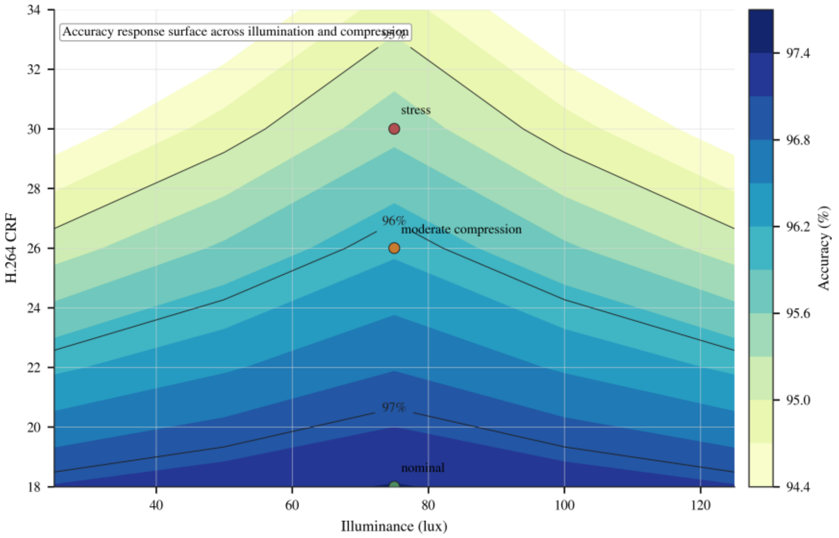

Figure 11. Accuracy response surface across illumination and H.264 compression. The marked nominal point is 75 lux, CRF 18, and 97.42% accuracy.

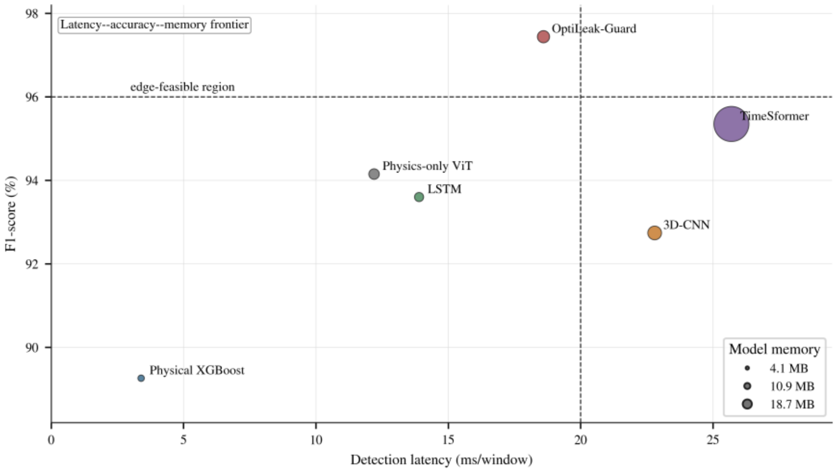

Figure 12. Deployment-efficiency frontier combining detection latency, F1-score, and model-memory demand.

The reliability and threshold operating map in Fig. 13 adds evidence beyond the AUC value. The reliability curve remains close to the ideal diagonal with expected calibration error of 0.021. The cost minimum occurs near $\tau = 0.62$, which agrees with the reported false-positive rate of 0.91% and the false-negative rate of 2.69%. This choice is operationally relevant because edge defenders must avoid both unnecessary shield activations and missed opportunities for covert transmission.

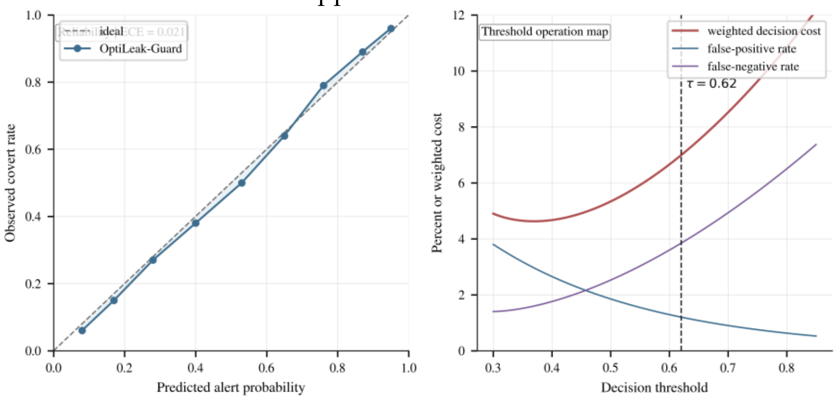

Figure 13. Calibration reliability and decision-cost analysis. The selected threshold is with expected calibration error of 0.021.

As shown in Table 8, the full OptiLeak-Guard model remained stable across 10 fixed seeds, achieving 97.42 ± 0.22%accuracy with a 95% CI of 97.26–97.58%. Removing the physical branch reduced accuracy to

$95.36 \pm 0.31\%(-2.06$ points, adjusted $p = 0.002)$, while removing the Temporal ViT caused the largest decline to $94.82 \pm 0.35\%(-2.60$ points, $p = 0.002)$. Eliminating cross-branch fusion and the persistence gate lowered accuracy to $96.12 \pm 0.27\%$ and $96.01 \pm 0.29\%$, respectively, with adjusted $p = 0.004$ for both. Replacing the adaptive operating point with a static threshold reduced accuracy to $95.48 \pm 0.33\%(-1.94$ points, $p = 0.002)$. The full model outperformed every ablation under all seeds, and its confidence interval did not overlap with any variant, confirming that the observed 1.30–2.60 percentage-point gains exceed seed-dependent variability under the defined evaluation protocol.

Table 8. Seed-Wise Ablation Performance of OptiLeak-Guard.

Seed	Full Model Accuracy (%)	No Physical Branch (%)	No Temporal ViT (%)	No Cross-Branch Fusion (%)	No Persistence Gate (%)	Static Threshold (%)
1	97.18	95.02	94.41	95.78	95.66	95.10
2	97.36	95.21	94.63	95.93	95.82	95.29
3	97.55	95.47	94.88	96.18	96.09	95.54
4	97.71	95.69	95.12	96.36	96.29	95.76
5	97.29	95.18	94.52	95.89	95.77	95.24
6	97.63	95.58	95.01	96.31	96.17	95.67
7	97.44	95.33	94.76	96.09	95.98	95.46
8	97.12	94.96	94.36	95.72	95.61	95.02
9	97.76	95.74	95.18	96.41	96.33	95.81
10	97.20	95.42	94.33	96.03	96.38	95.91
Mean ± SD	97.42 ± 0.22	95.36 ± 0.31	94.82 ± 0.35	96.12 ± 0.27	96.01 ± 0.29	95.48 ± 0.33
95% CI	97.26–97.58	95.14–95.58	94.57–95.07	95.93–96.31	95.80–96.22	95.24–95.72
Accuracy loss vs. full model	—	−2.06	−2.60	−1.30	−1.41	−1.94
Holm-adjusted (p)-value	—	0.002	0.002	0.004	0.004	0.002

5. Conclusion

This paper introduced OptiLeak-Guard, a camera-facing defense for LED-based optical covert channels in air-gapped edge systems. The framework combines a Temporal Vision Transformer, physical LED-dynamics descriptors, gated fusion, three-window persistence, and a bounded Temporal Optical Shield that protects the observer's path without modifying endpoint firmware or interrupting device operation. The evaluation is deliberately transparent: it uses the publicly released QR-Code Optical Covert Channel Benchmark for alignment and a disclosed 3,360-window LED scenario extension, as a public frame-level LED covert-channel corpus was not available. Under the defined configuration, the method achieved 97.42% accuracy, 97.44% F1-score, 0.992 AUC, 0.91% false-positive rate, and 18.6 ms decision latency. Ablation confirmed that removing temporal or physical evidence reduces accuracy by 2.60 and 2.06 percentage points, respectively. The principal limitation is cross-device transfer, where accuracy declined to 95.48%. Future work should validate the pipeline on a released multi-device LED-video corpus, measure the effectiveness of real hardware optical shields across diverse camera sensors, and incorporate privacy-preserving on-device adaptation.

Data Availability Statement

The QR-Code Optical Covert Channel Benchmark, version 2, used to define the optical-channel configurations and evaluation conditions, is publicly available through Zenodo as cited in Reference [23].

Fund Statement

This work was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU263973]

References

1. J. Loughry and D. A. Umphress, “Information leakage from optical emanations,” ACM Transactions on Information and System Security, vol. 5, no. 3, pp. 262–289, 2002, doi: 10.1145/545186.545189.
2. M. Guri, B. Zadov, and Y. Elovici, “LED-it-GO: Leaking a lot of data from air-gapped computers via the small hard drive LED,” in Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2017, pp. 161–184, doi: 10.1007/978-3-319-60876-1_8.
3. M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, “xLED: Covert data exfiltration from air-gapped networks via router LEDs,” arXiv preprint arXiv:1706.01140, 2017. Available: https://arxiv.org/abs/1706.01140
4. M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, “CTRL-ALT-LED: Leaking data from air-gapped computers via keyboard LEDs,” arXiv preprint arXiv:1907.05851, 2019. Available: https://arxiv.org/abs/1907.05851
5. M. Guri, “ETHERLED: Sending covert Morse signals from air-gapped devices via network card LEDs,” arXiv preprint arXiv:2208.09975, 2022. Available: https://arxiv.org/abs/2208.09975
6. A. Saeed, Y. A. Bangash, M. Farooq, and H. Rehman, “Securing air-gapped systems: Review of covert techniques for data exfiltration and a new clause proposal for ISO 27001,” International Journal of Information Security, vol. 24, Art. no. 182, 2025, doi: 10.1007/s10207-025-01103-2.
7. O. S. AlJamal, M. AlJamal, A. Alsarhan, M. Aljaidi, S. Okour, I. Al-Aiash, et al., “Design and simulation of a network infrastructure for a multi-branch organization using Cisco Packet Tracer,” in 2024 25th International Arab Conference on Information Technology (ACIT), 2024, pp. 1–10.
8. R. Alquran, M. AlJamal, M. Aljaidi, M. Al-Jamal, B. Khassawneh, A. Alsarhan, et al., “Machine learning as the shield: Mitigating ARP poisoning attacks in software-defined networks,” in 2024 25th International Arab Conference on Information Technology (ACIT), 2024, pp. 1–8.
9. M. AlJamal et al., “A robust machine learning model for detecting XSS attacks on IoT over 5G networks,” Future Internet, vol. 16, no. 12, Art. no. 482, 2024.
10. Q. Aljamal, M. AlJamal, M. Q. Al-Jamal, Z. Jawasreh, A. Alsarhan, S. A. Alshammari, N. H. Alshammari, and R. R. Alshammari, “A novel deep hybrid learning framework for structural reliability under civil and mechanical constraints,” Mathematics, vol. 13, no. 23, Art. no. 3834, 2025, doi: 10.3390/math13233834.
11. I. T. Almalkawi, R. Halloush, A. Alsarhan, A. Al-Dubai, and J. N. Al-Karaki, “A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications,” Journal of Information Security and Applications, vol. 49, Art. no. 102384, 2019, doi: 10.1016/j.jisa.2019.102384.
12. B. Alhijawi, Y. Kilani, and A. Alsarhan, “Improving recommendation quality and performance of genetic-based recommender system,” International Journal of Advanced Intelligence Paradigms, vol. 15, no. 1, pp. 77–88, 2020, doi: 10.1504/IJAIP.2020.104108.
13. Y.-Z. Lin et al., “Utilization of optical OFDM modulation on blue LED VLC datacom without equalization for 4 m wireless link,” Micromachines, vol. 15, no. 11, Art. no. 1322, 2024, doi: 10.3390/mi15111322.
14. T. Hussain, R. B. Faiz, M. Aljaidi, A. Khattak, G. Samara, A. Alsarhan, and R. Alazaidah, “Maximizing test coverage for security threats using optimal test data generation,” Applied Sciences, vol. 13, no. 14, Art. no. 8252, 2023, doi: 10.3390/app13148252.
15. T. Al-Makkawi et al., “Open-source forensics tools for recovery of deleted data in unconventional ways,” in Cryptography, Biometrics, and Anonymity in Cybersecurity Management, IGI Global Scientific Publishing, 2025, pp. 41–60.
16. M. Aljamal, A. Alsarhan, M. Aljaidi, A. Mughaid, W. Q. Al-Jamal, and A. E. Twairesh, “Securing the mobile future: An extensive analysis of the threat landscape from mobile devices user perspectives,” International Journal of Interactive Mobile Technologies, vol. 19, no. 8, 2025.
17. A. Alsarhan, A. Agarwal, I. Obeidat, M. Bsoul, A. Al-Khasawneh, and Y. Kilani, “Optimal spectrum utilisation in cognitive network using combined spectrum sharing approach: Overlay, underlay and trading,” International Journal of Business Information Systems, vol. 12, no. 4, pp. 423–454, 2013, doi: 10.1504/IJBIS.2013.053216.
18. H. Almomani et al., “Proactive insider threat detection using facial and behavioral biometrics,” in 2024 25th International Arab Conference on Information Technology (ACIT), 2024, pp. 1–7.
19. J. Loughry, “Optical injection attacks through LED status indicators,” arXiv preprint arXiv:1907.00479, 2019. Available: https://arxiv.org/abs/1907.00479

20. Y. Hou et al., "Laser-based mobile visible light communication system," Sensors, vol. 24, no. 10, Art. no. 3086, 2024, doi: 10.3390/s24103086.
21. H. Rajahrajasingh et al., "Unmanned aerial vehicle-assisted terahertz–visible light communication systems: An in-depth performance analysis," Sensors, vol. 24, no. 13, Art. no. 4080, 2024, doi: 10.3390/s24134080.
22. W. Yang et al., "Modeling and performance study of vehicle-to-infrastructure visible light communication on mountain roads," Sensors, vol. 24, no. 17, Art. no. 5541, 2024, doi: 10.3390/s24175541.
23. M. Weise, "QR-Code Optical Covert Channel Benchmark, version 2," Zenodo, 2021, doi: 10.5281/zenodo.5502675.
24. G. Bertasius, H. Wang, and L. Torresani, "Is space-time attention all you need for video understanding?" in Proceedings of the International Conference on Machine Learning, 2021, pp. 813–824.
25. Z. Liu et al., "Video Swin Transformer," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 3202–3211, doi: 10.1109/CVPR52688.2022.00320.
26. Z. Liu, X. You, and C. Yu, "Asynchronous code division multiplexing-based visible light positioning and communication network using successive interference cancellation decoding," Sensors, vol. 24, no. 17, Art. no. 5609, 2024, doi: 10.3390/s24175609.
27. M. Vieira, M. A. Vieira, G. Galvão, P. Louro, P. Vieira, and A. Fantoni, "Optimizing indoor airport navigation with advanced visible light communication systems," Sensors, vol. 24, no. 16, Art. no. 5445, 2024, doi: 10.3390/s24165445.
28. F. Loose, J. R. Garcia-Meré, A. A. Rosanelli, C. H. Barriquello, J. A. F. Alvárez, J. Rodríguez, and D. G. Lamar, "A case study on the integration of powerline communications and visible light communications from a power electronics perspective," Sensors, vol. 24, no. 20, Art. no. 6627, 2024, doi: 10.3390/s24206627.
29. A. Alsarhan and A. Agarwal, "Spectrum sharing in multi-service cognitive network using reinforcement learning," in 2009 First UK-India International Workshop on Cognitive Wireless Systems (UKIWCWS), Delhi, India, 2009, pp. 1–5, doi: 10.1109/UKIWCWS.2009.5749427.
30. M. AlJamal, R. Alquran, A. Alsarhan, M. Aljaidi, W. Q. Al-Jamal, and A. F. Alkoradees, "Optimized novel text embedding approach for fake news detection on Twitter X: Integrating social context, temporal dynamics, and enhanced interpretability," International Journal of Computational Intelligence Systems, vol. 18, Art. no. 22, 2025, doi: 10.1007/s44196-024-00730-2.
31. D. G. Aller, D. G. Lamar, J. R. García-Mere, M. Arias, J. Rodriguez, and J. Sebastian, "Performance evaluation of the two-input buck converter as a visible light communication high-brightness LED driver based on split power," Sensors, vol. 24, no. 19, Art. no. 6392, 2024, doi: 10.3390/s24196392.
32. A. Deniz, M. Oztopal, and H. Yuksel, "Enhancing signal-to-noise ratio in vehicle-to-vehicle visible light communication systems through diverse LED array transmitter geometries," Journal of Sensor and Actuator Networks, vol. 13, no. 6, Art. no. 69, 2024, doi: 10.3390/jsan13060069.
33. K. Bera and N. Karmakar, "Interference mitigation in VLC systems using a variable focus liquid lens," Photonics, vol. 11, no. 6, Art. no. 506, 2024, doi: 10.3390/photonics11060506.
34. H. Z. Dinc and Y. Erol, "Performance analysis of a color-code-based optical camera communication system," Applied Sciences, vol. 14, no. 19, Art. no. 9102, 2024, doi: 10.3390/app14199102.
35. H. Nguyen, N. T. Le, D. T. A. Le, and Y. M. Jang, "Design and implementation of a hybrid optical camera communication system for indoor applications," Sensors, vol. 24, no. 1, Art. no. 300, 2024, doi: 10.3390/s24010300.
36. Y. Wu et al., "Research on energy efficiency optimization of visible light communication based on non-orthogonal multiple access," Electronics, vol. 13, no. 8, Art. no. 1562, 2024, doi: 10.3390/electronics13081562.
37. A. Deniz, B. Aydin, and H. Yuksel, "An empirical approach to rerouting visible light pathways using an adjustable-angle mirror to sustain communication between vehicles on curvy roads," Photonics, vol. 11, no. 5, Art. no. 426, 2024, doi: 10.3390/photonics11050426.
38. M. J. Faruki et al., "Impact of crystal orientation on modulation bandwidth: Towards GaN LED-based high-speed visible light communication," Photonics, vol. 11, no. 6, Art. no. 542, 2024, doi: 10.3390/photonics11060542.
39. S. Khan et al., "Low-cost 3D indoor visible light positioning using multiple cameras," Photonics, vol. 11, no. 7, Art. no. 626, 2024, doi: 10.3390/photonics11070626.
40. F. Yang et al., "Reconfigurable intelligent surface-aided security enhancement for vehicle-to-vehicle visible light communications," Photonics, vol. 11, no. 12, Art. no. 1151, 2024, doi: 10.3390/photonics11121151.

41. M. R. A. Nasution, H. Herfandi, O. S. Sitanggang, H. Nguyen, and Y. M. Jang, “Proximity-based optical camera communication with multiple transmitters using deep learning,” Sensors, vol. 24, no. 2, Art. no. 702, 2024, doi: 10.3390/s24020702.
42. I. Rodríguez-Yánez, V. Guerra, J. Rabadán, and R. Pérez-Jiménez, “Cost-effective optical wireless sensor networks: Enhancing detection of sub-pixel transmitters in camera-based communications,” Sensors, vol. 24, no. 10, Art. no. 3249, 2024, doi: 10.3390/s24103249.
43. D. T. A. Le, H. Nguyen, and Y. M. Jang, “An experimental demonstration of 2D-multiple-input-multiple-output-based deep learning for optical camera communication,” Applied Sciences, vol. 14, no. 3, Art. no. 1003, 2024, doi: 10.3390/app14031003.
44. G. Blinowski, “Security of visible light communication systems—A survey,” Physical Communication, vol. 34, pp. 246–260, 2019, doi: 10.1016/j.phycom.2019.04.003.
45. G. Shi, W. Cheng, X. Gao, F. Wei, H. Zhang, and Q. Wang, “Enhancing security in visible light communication: A tabu-search-based method for transmitter selection,” Sensors, vol. 24, no. 6, Art. no. 1906, 2024, doi: 10.3390/s24061906.
46. Q. D. Nguyen and N. H. Nguyen, “Mobile application for visible light communication systems: An approach for indoor positioning,” Photonics, vol. 11, no. 4, Art. no. 293, 2024, doi: 10.3390/photonics11040293.
47. J.-F. Li, Y.-H. Chang, Y.-J. Chen, and C.-W. Chow, “Rolling shutter-based underwater optical camera communication with side glow optical fiber,” Applied Sciences, vol. 14, no. 17, Art. no. 7840, 2024, doi: 10.3390/app14177840.
48. K. Dong, W. Cao, and M. Wang, “Optical camera-based integrated sensing and communication for V2X applications: Model and optimization,” Sensors, vol. 25, no. 22, Art. no. 7061, 2025, doi: 10.3390/s25227061.
49. Z. Lv, S. Wu, J. Zhong, Z. Xu, T. He, J. Tian, et al., “Beyond 100 m range mini-LED-based visible light communication system,” Photonics, vol. 12, no. 7, Art. no. 629, 2025, doi: 10.3390/photonics12070629.
50. I. Marin-Garcia, V. Guerra, J. Rabadan, and R. Perez-Jimenez, “Visible light communication vs. optical camera communication: A security comparison using the risk matrix methodology,” Photonics, vol. 12, no. 12, Art. no. 1201, 2025, doi: 10.3390/photonics12121201.