photonics

MDPI

Article

Visible Light Communication vs. Optical Camera Communication: A Security Comparison Using the Risk Matrix Methodology

Ignacio Marin-Garcia [1,2,†], Victor Guerra [3,*,†], Jose Rabadan [2,†] and Rafael Perez-Jimenez [2,†]

[1] Department of Telematics, Escuela Superior Politecnica del Litoral, Guayaquil 090112, Ecuador; imaringa@espol.edu.ec
[2] IDeTIC, Universidad de las Palmas de Gran Canaria, 35001 Las Palmas de Gran Canaria, Spain; jose.rabadan@ulpgc.es (J.R.); rafael.perez@ulpgc.es (R.P.-J.)
[3] Wooptix S.L., 38204 La Laguna, Spain
* Correspondence: victor.guerra@wooptix.com
† These authors contributed equally to this work.

Abstract

Optical Wireless Communication (OWC) technologies are emerging as promising complements to radio-frequency systems, offering high bandwidth, spatial confinement, and license-free operation. Within this domain, Visible Light Communication (VLC) and Optical Camera Communication (OCC) represent two distinct paradigms with divergent performance and security profiles. While VLC leverages LED-photodiode links for high-speed data transfer, OCC exploits ubiquitous image sensors to decode modulated light patterns, enabling flexible but lower-rate communication. Despite their potential, both remain vulnerable to various attacks, including eavesdropping, jamming, spoofing, and privacy breaches. This work applies—and extends—the Risk Matrix (RM) methodology to systematically evaluate the security of VLC and OCC across reconnaissance, denial, and exploitation phases. Unlike prior literature, which treats VLC and OCC separately and under incompatible threat definitions, we introduce a unified, domain-specific risk framework that maps empirical channel behavior and attack feasibility into a common set of impact and likelihood indices. A normalized risk rank (NRR) is proposed to enable a direct, quantitative comparison of heterogeneous attacks and technologies under a shared reference scale. By quantifying risks for representative threats—including war driving, Denial of Service (DoS) attacks, preshared key cracking, and Evil Twin attacks—our analysis shows that neither VLC nor OCC is intrinsically more secure; rather, their vulnerabilities are context-dependent, shaped by physical constraints, receiver architectures, and deployment environments. VLC tends to concentrate confidentiality-driven exposure due to optical leakage paths, whereas OCC is more sensitive to availability-related degradation under adversarial load. Overall, the main contribution of this work is the first unified, standards-aligned, and empirically grounded risk-assessment framework capable of comparing VLC and OCC on a common security scale. The findings highlight the need for technology-aware security strategies in future OWC deployments and demonstrate how an adapted RM methodology can identify priority areas for mitigation, design, and resource allocation.

Keywords: VLC; OCC; OWC; risk matrix; security assessment

Received: 30 September 2025
Revised: 27 November 2025
Accepted: 1 December 2025
Published: 5 December 2025

Citation: Marin-Garcia, I.; Guerra, V.; Rabadan, J.; Perez-Jimenez, R. Visible Light Communication vs. Optical Camera Communication: A Security Comparison Using the Risk Matrix Methodology. *Photonics* **2025**, *12*, 1201. https://doi.org/10.3390/photonics12121201

1. Introduction

Wireless communication systems have revolutionized the exchange of information, enabling applications across virtually every sector; this pervasive connectivity comes at

the cost of increased vulnerability. Attacks such as eavesdropping, Denial of Service (DoS), spoofing, and key cracking are recurrent threats in Radio Frequency (RF) and Wireless Local Area Networks (WLANs), raising serious concerns about the confidentiality, integrity, and availability of transmitted data [1,2].

Optical Wireless Communication (OWC) technologies have emerged as promising alternatives or complements to RF-based systems. By using light as the communication medium, they offer benefits such as license-free operation, inherent spatial confinement, and high bandwidth [3]. However, the security of OWC systems is far from guaranteed. Several works have demonstrated that, despite their physical confinement, OWC systems remain susceptible to attacks, including side-channel eavesdropping through reflective surfaces, light jamming, and impersonation [4,5].

Within the OWC paradigm, Optical Camera Communication (OCC) is gaining attention as a support technology for 6G networks. OCC leverages ubiquitous camera sensors to receive data transmitted via modulated light, typically from Light Emitting Diodes (LEDs) or screens [6]. Compared to other OWC technologies such as Visible Light Communication (VLC) or Li-Fi, OCC presents several potential a priori security advantages:

- It enables asymmetric communication. Emitters can be simple LEDs while receivers (cameras) process complex signals.
- It benefits from spatial filtering, which may reduce exposure to side-channel attacks.
- It allows source localization and frame-by-frame validation using visual context, potentially improving spoofing detection.

Despite these advantages, OCC is not inherently secure. The camera-based reception model introduces unique vulnerabilities that adversaries can exploit. For instance, malicious actors may employ visual jamming techniques to deliberately saturate or blind the image sensor, thereby disrupting communication. Similarly, spoofed pattern injections can deceive the receiver by projecting crafted optical signals that mimic legitimate data, compromising both integrity and authenticity [7]. In addition, the inherently wide Field-of-View (FoV) of cameras makes OCC highly sensitive to environmental interference (e.g., ambient light fluctuations, reflections) and unintended capture of extraneous sources, which can degrade performance a and reflections) and to ncerns [5]. As deployment scenarios grow more complex—ranging from vehicle-to-infrastructure to dense Internet of Things (IoT) environments—the need for systematic, technology-aware security assessment becomes increasingly pressing.

The Risk Matrix (RM) methodology provides a structured, practical approach to evaluating the security of emerging communication technologies. Though its roots lie in military and industrial safety contexts, where risk to lives, infrastructure, and mission-critical systems must be quantitatively and qualitatively assessed, the RM framework has since been adopted across many sectors for evaluating cybersecurity and emerging technological threats [8]. Within RM, threats are assessed along two essential axes: the impact of a successful attack (how severe its consequences would be) and the likelihood of its occurrence (how probable the attack is under realistic conditions). This two-dimensional view enables decision-makers to prioritize mitigation measures, even when comprehensive empirical data on attacks are scarce. Light-based wireless systems, such as OCC or VLC, are excellent candidates for this kind of analysis, as they are still relatively early in their deployment, with limited commercial exposure, but face a diversity of possible vulnerabilities. In such settings, RM offers a realistic and scalable framework for assessing and comparing risks based on expert judgment and scenario-based modeling, thereby guiding resource allocation and design trade-offs [3,9].

The motivation for this study is the need for a unified, reproducible framework to assess the security posture of heterogeneous optical wireless systems. Traditional metrics, such as bit-error rate or channel capacity, are insufficient to capture the human- and system-

level consequences of attacks. The RM methodology offers a complementary perspective by linking measurable technical factors to their operational impact and likelihood. This approach enables comparative reasoning between technologies that differ fundamentally in architecture—such as VLC and OCC—and allows system designers to quantify vulnerabilities and prioritize mitigation efforts even in the absence of extensive experimental data. Ultimately, adopting RM as a security analysis tool improves the reliability and resilience of optical wireless networks by revealing the trade-offs among confidentiality, availability, and implementation complexity that shape their real-world deployment.

Contributions of this work.Unlike prior studies that examine VLC and OCC separately, this paper provides the first unified and technology-aware security comparison of both systems under a consistent methodological framework. The main contributions are as follows:

- Unified security assessment framework: We extend the RM methodology with a harmonized set of impact and likelihood indices that apply to both VLC and OCC, despite their fundamentally different physical layers and receiver architectures.
- Domain-specific adaptation of the RM: We introduce technology-aware corrections and asymmetric factors—such as feasibility, detectability, channel exposure, and recovery effort—that are tailored to optical wireless systems and not present in generic ISO/IEC 27005 [10] implementations.
- Normalized Risk Rank (NRR): We propose a normalization procedure that enables direct, quantitative comparison of heterogeneous threats and technologies under a standard reference scale, avoiding arbitrary or technology-specific scoring.
- Unified threat modeling: We reconstruct representative attacks (war driving, DoS, pre-shared key cracking, and Evil Twin attacks) under a single cross-technology definition, allowing direct comparison of their risk profiles for the first time.
- Security insights for deployment: Our analysis reveals a structural asymmetry between both technologies: VLC concentrates confidentiality-driven exposure due to optical leakage and reflective paths, while OCC is more vulnerable to availability degradation under adversarial load. These insights translate directly into technology-aware design guidelines for future OWC deployments.

To avoid any misunderstanding, we emphasize that this work does not apply the Risk Matrix as a generic management tool. Instead, it redefines and extends the RM specifically for optical wireless security by introducing new OWC-specific indices, normalization procedures, and a unified cross-technology evaluation framework unavailable in standard ISO/IEC 27005 [10] formulations. This makes the methodology itself a core part of the scientific contribution.

To the best of our knowledge, no existing VLC or OCC security study provides a unified, reproducible, and quantitatively comparable risk framework across optical wireless technologies. Previous works analyse threats in isolation, using incompatible assumptions and non-harmonized risk scales, which makes cross-technology security evaluation impossible. The present study directly addresses this gap by offering the first harmonized, technology-independent formulation for comparing VLC and OCC on a consistent methodological foundation.

The rest of the paper is organized as follows. Section 2 presents the theoretical framework of VLC and OCC technologies. Section 3 reviews the current literature on their respective vulnerabilities. Section 4 details the RM methodology used in this analysis. Section 5 discusses the findings based on our evaluation. Finally, Section 6 concludes the paper and outlines future research directions.

2. Theoretical Framework on Visible-Light Optical Wireless Technologies

Before assessing the security risks of OWC technologies using the RM methodology, it is essential to establish a solid theoretical foundation for the systems under comparison. This section presents the technical architecture, communication principles, and operational characteristics of VLC and OCC systems, which represent two major paradigms within the OWC domain. Emphasis is placed on features that directly influence their respective security postures, such as transmission mechanisms, hardware constraints, and environmental dependencies. Furthermore, we provide a comparative overview of attack surfaces inherent to each technology, identifying potential vulnerabilities and system-level implications. This groundwork serves to motivate the application of the RM as a suitable framework to assess security in the absence of large-scale empirical data and to guide decision-making in future deployments.

2.1. VLC Systems Overview

Figure 1 illustrates representative architectures of both VLC and OCC systems, used as a common reference for the comparative analysis presented in this work.

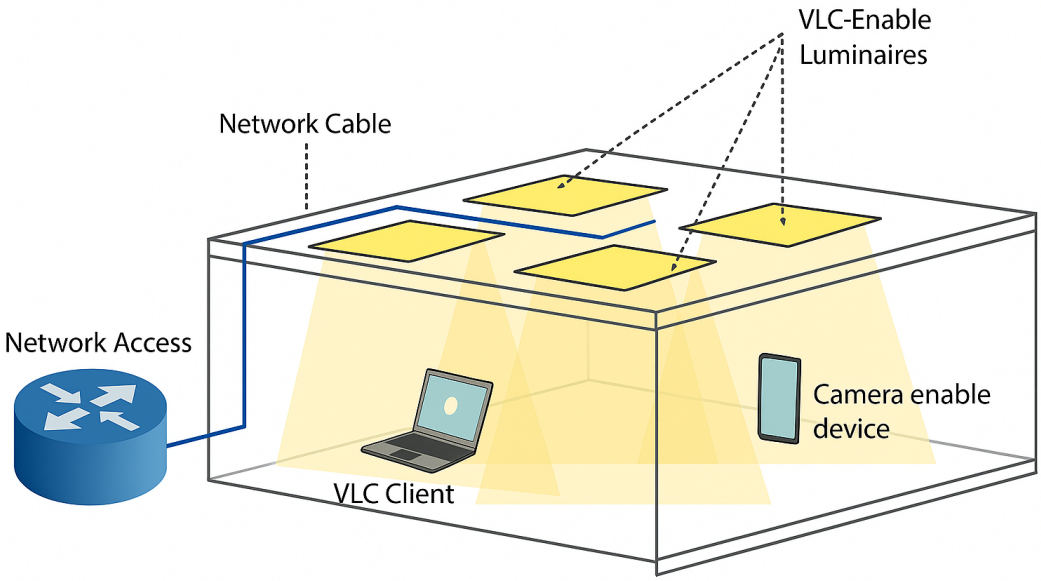

Figure 1. Representative architectures of VLC and OCC systems. Ceiling-mounted VLC-enabled luminaires provide both illumination and data transmission. The VLC Client (laptop) uses photodiode-based reception, while the Camera-enabled device (smartphone) exemplifies an OCC receiver that decodes modulated light via an image sensor. Both systems share network connectivity via a common infrastructure.

VLC offers several attractive features from both performance and security perspectives:

- High bandwidth: Theoretically, LEDs can be modulated at MHz rates (except Chip-On-Board devices or very large flip-chip LEDs), supporting fast data transmission without electromagnetic interference.
- Spatial confinement: Light does not penetrate opaque objects, limiting unintentional signal leakage beyond walls.
- Dual use: VLC enables data transmission using infrastructure already in place for illumination, maximizing energy efficiency and spatial reuse.
- Positioning capabilities: The spatially bounded nature of light allows for high-resolution indoor positioning by triangulating signals from multiple luminaires.

Despite its potential, VLC systems face several limitations such as:

- Line-of-Sight (LoS) dependency: VLC requires a mostly unobstructed path between the LED and the receiver to maintain data integrity.
- Limited mobility: Fast movement or occlusion can severely degrade performance, making it unsuitable for highly dynamic environments without redundancy.
- Limited practical data rates: Achieving high-throughput VLC links remains challenging in real-world deployments, as the design requirements for lighting and communication are often conflicting. While luminaires typically use large arrays of series-connected LEDs to balance luminous efficiency and fault tolerance, such configurations introduce parasitic capacitance that limits modulation bandwidth. To enable high-speed communication, emitters must be partially decoupled, which increases circuit complexity and compromises lighting uniformity.
- Susceptibility to ambient light: Photodiodes may saturate or misinterpret signals in the presence of sunlight or fluorescent flickering.
- Synchronization complexity: Modulation schemes must remain imperceptible to the human eye while enabling high-speed decoding, which imposes technical constraints on both transmitter and receiver design.

These developments have pushed VLC closer to becoming a versatile wireless access technology. However, its performance and security depend heavily on deployment geometry, optical channel characteristics, and user mobility patterns. These aspects will be central when comparing VLC to camera-based OWC paradigms in later sections. (Additional implementation parameters and physical-layer details are provided in Appendix A.).

2.2. OCC Systems Overview

OCC is an emerging modality within the OWC family that uses image sensors—typically found in commercial Complementary Metal–Oxide–Semiconductor (CMOS) cameras—to receive modulated optical signals from LED-based emitters or display screens. In contrast to VLC, which relies on analog photodetectors and continuous signal reception, OCC employs discrete frame capture and digital image processing to extract embedded information from spatiotemporal light patterns.

Figure 1 illustrates a typical OCC configuration, where an LED array transmits data to a receiving camera with a defined FoV. The transmission can occur using visible or near-infrared light, and in both LoS and No-Line-of-Sight (NLoS) scenarios, depending on the camera's spatial setup and resolution.

OCC introduces several benefits that distinguish it from other OWC systems:

- Ubiquitous hardware: Most smartphones, tablets, and embedded devices already include cameras, enabling cost-effective adoption without additional receivers.
- Asynchronous reception: Cameras operate independently from the emitter's clock, removing the need for tight synchronization.
- Spatial multiplexing and visual context: OCC receivers can simultaneously capture multiple transmitters within a single frame. They can use surrounding visual cues to verify signal origin or detect spoofing.
- Inherent directionality: The narrow FoV of many lenses acts as a physical filter against off-axis interference or jamming.

Despite its promise, OCC has several technical limitations, among which we must highlight:

- Frame-rate bottlenecks: The achievable data rate is fundamentally constrained by the frame acquisition speed, especially in low-end or general-purpose cameras.
- Processing overhead: Extracting data from images involves intensive decoding and filtering operations, which can increase latency and drain battery resources.

- Sensitivity to ambient light and motion blur: Exposure to bright backgrounds, flickering sources, or fast movement can degrade image quality and reduce decoding reliability.
- Uncertainty in alignment: Cameras must be oriented appropriately to capture the emitter within the FoV; minor angular deviations or occlusions can disrupt communication.

While VLC is often integrated into ceiling-mounted infrastructure for continuous coverage, OCC systems are typically user-centric, operating opportunistically via handheld devices or stationary surveillance systems. This decentralized nature, combined with greater variability in camera parameters (i.e., frame rate, shutter type, lens geometry), has hindered OCC's standardization and commercial scaling. Unlike VLC, OCC has not yet converged toward a unified physical layer or reference hardware platform, which limits interoperability and robustness in diverse environments.

Compared to VLC, OCC operates under fundamentally different assumptions. It relies on passive frame capture and digital post-processing rather than continuous analog reception. This frame-based architecture, along with its hybrid sensing and communication nature, significantly impacts both system performance and security exposure. The following subsection compares VLC and OCC at a structural level, highlighting how their distinct physical layers translate into different vulnerability profiles and defensive opportunities.

2.3. Comparison Between Technologies

VLC and OCC share a common optical foundation within the OWC paradigm. Still, they diverge significantly in terms of their transceiver architecture, channel dynamics, performance capabilities, and security posture.

VLC relies on the modulation of visible light intensity emitted by LED arrays, typically decoded via analog photodiodes using Intensity Modulation with Direct Detection (IM/DD). This setup enables high-speed, low-latency data transfer in short-range environments, benefiting from well-characterized opticadiffer significantly in systems modulate light to embed data within visual patterns that are captured and decoded by CMOS cameras. Two primary OCCmodulating the intensity of visible light emitted by LED arrays, typically decoded bye sequential scanning behavior of image sensors to achieve higher effective symbol rates [11], and Global Shutter (GS)-based systems, which are frame rate limited but offer more uniform sampling [12]. An additional regime—sub-pixel OCC—emerges when the emitter projects to a spatial footprint smaller than a single pixel, enabling long-range communication with advanced decoding strategies [13].

From a Physical Layer perspective, VLC emphasizes optimized emitter-receiver alignment, requiring near-LoS conditions and stable illumination geometries. The receiver's FoV is typically wide and non-discriminative, making VLC vulnerable to overlapping emitters unless managed through careful spatial and spectral filtering. OCC, by contrast, is inherently directional: the receiving camera can selectively decode specific regions within its FoV, enabling robust spatial multiplexing but at the cost of lower throughput and increased computational load due to frame-based image processing.

Security vulnerabilities in both technologies stem from their reliance on visible light propagation, but the attack surfaces differ. VLC benefits from its spatial confinement; walls and opaque barriers effectively block light, limiting exposure to outside threats. However, when attackers gain physical access or line-of-sight proximity, eavesdropping and DoS attacks via optical jamming remain viable threats. Moreover, the low diversity in receiver types (mostly standard photodiodes) limits the potential for advanced in-channel authentication or interference mitigation.

On the other hand, OCC presents a richer yet more complex security landscape. The use of cameras as receivers introduces susceptibility to optical jamming, signal spoofing, and interference from ambient light. For instance, an adversary could inject misleading

visual patterns into the camera's FoV or use high-intensity sources to saturate the image sensor. The variability in optical channels caused by reflections, occlusions, or motion blur adds further unpredictability. However, this same visual richness can be harnessed defensively: image-based anomaly detection and spatial filtering can be used to validate signal integrity or discard tampered regions. Thus, OCC may offer unique security mitigation mechanisms unavailable to VLC, albeit with greater implementation complexity.

In summary, while both VLC and OCC share some common vulnerabilities, notably eavesdropping and DoS, their respective architectures create distinct attack vectors and defensive capabilities. VLC is constrained by physical geometry and lighting infrastructure, whereas OCC systems face challenges tied to optical capture, sensor response, and environmental variability. These contrasts justify a differentiated security assessment, which is addressed in Section 4 using the RM methodology.

3. Related Work

VLC and OCC are two complementary technologies under the broader OWC paradigm. Both leverage visible light as the transmission medium but differ significantly in architecture, performance, and security exposure. VLC typically employs high-speed LEDs as transmitters and photodiodes as receivers, allowing data rates in the Mbps to Gbps range. In contrast, OCC uses image sensors—such as CMOS cameras—to receive light signals, offering greater flexibility at the cost of lower bandwidth.

Several studies have investigated security vulnerabilities in VLC and OCC, addressing their susceptibility to eavesdropping, spoofing, DoS, and privacy leakage. In VLC, the widespread belief is that its high directionality and LoS requirement act as inherent security features. However, extensive research challenges this assumption. For instance, Younus et al. [14] and Zhang et al. [15] demonstrated that VLC links are not immune to eavesdropping; adversaries can intercept signals via indirect reflections, particularly with the use of high-gain photodetectors. Similarly, Koale et al. [16] and Huang et al. [17] exposed the vulnerability of VLC links to Physical Layer attacks, highlighting that even systems relying on visible light are not exempt from classical wireless security threats. Recent surveys, such as Zhang et al. [3], further categorize OWC threats into distinct stages (pre-transmission, propagation, and post-reception), confirming that vulnerabilities are systemic and not limited to specific layers. Furthermore, works [18–20] further validate these risks, demonstrating practical eavesdropping and data interception scenarios over VLC channels.

To address these concerns, various Physical Layer (PHY) countermeasures have been proposed. Arfaoui et al. [21] introduced a secure modulation scheme based on orthogonal frequency division multiplexing (OFDM) with artificial noise, increasing the secrecy capacity of VLC channels. Su et al. [22] explored spatial beamforming and directional LED emission to reduce information leakage. Other PHY-level techniques include Code Division Multiple Access (CDMA) with optical orthogonal codes [23] and color-shift keying with hyperchaotic maps for secure symbol encoding [24,25]. More recent proposals exploit intelligent reflecting surfaces (IRS) to enhance secrecy rates in VLC [26,27], or even IRS-aided jamming strategies for 6G-oriented networks [28]. These approaches demonstrate that PHY-centric security in VLC can significantly mitigate interception risk, but often at the cost of system complexity and energy efficiency.

At the protocol and application layer, further enhancements have been suggested. Nguyen et al. [29] studied hybrid systems combining VLC and OCC, suggesting that dual-modality transmission can increase resilience against single-channel vulnerabilities. Koale et al. [16] proposed a lightweight key exchange protocol adapted for constrained VLC systems. Additionally, Abuella et al. [30] demonstrated that hybrid VLC/RF systems present unique challenges for optimizing the secrecy rate in cooperative networks.

In parallel, OCC-specific security studies have gained traction. Due to its reliance on cameras, OCC is vulnerable to spoofing, visual jamming, and unintentional privacy breaches. Saeed et al. [23] demonstrated that rolling shutter mechanisms can be exploited for asynchronous spoofing attacks. Koale et al. [16] showed how OCC receivers could be tricked via screen-based replay attacks, particularly in public or crowded environments. Kazik et al. [31] examined the difficulty of authenticating OCC sources due to the lack of consistent signal patterns and tight synchronization, recommending signal fingerprinting as a countermeasure. More broadly, Zhang et al. [15] summarize practical OCC limitations—low Signal-to-Noise Ratio (SNR), background light interference, Region of Interest (ROI) extraction—which directly impact the robustness of security mechanisms.

Despite the proliferation of security-oriented proposals, the literature remains fragmented. While most studies provide proof-of-concept demonstrations or protocol-level recommendations, few evaluate security from a systems-level or deployment-oriented perspective. The assumptions regarding eavesdropping difficulty, LOS dependency, and privacy exposure are often inconsistent or invalidated. For example, although VLC is assumed to be directionally confined, experimental studies by Younus et al. [14] and Zhang et al. [15] confirm that reflections and multipath propagation can expose side channels. Likewise, OCC's supposed advantage in user accessibility introduces new security risks, such as stealth signal capture and ambient spoofing, which are often underestimated in practical scenarios.

Table 1 synthesizes commonly assumed and verified security characteristics for both VLC and OCC systems. The comparison reveals substantial differences in signal confinement, data integrity, privacy risk, and the feasibility of authentication mechanisms.

Table 1. Common expectations of security features in VLC and OCC. Based on [3,15,16,23–33].

Security Feature	VLC	OCC
LOS Dependency	High (signal confined to illuminated area)	Moderate–High (susceptible to indirect capture)
Eavesdropping Risk	Low, but possible via reflections [32]	Moderate to high (wide FoV and long range)
Signal Leakage	Minimal due to focused LED beams	Higher due to broader emitting surfaces
Interference Resistance	Strong with filtering and modulation	Weaker; affected by ambient light and clutter
Authentication Feasibility	High (supports PHY/MAC cryptographic methods)	Limited (due to latency and bandwidth)
Spoofing Vulnerability	Difficult without replacing LED source	Easy via screen/ light imitation
DoS Susceptibility	Yes (via LED jamming or light flooding)	Yes (via visual overexposure or flash)
Data Integrity Risk	Low (FEC and modulation robust to noise)	Higher (motion blur, artifacts)
Privacy Exposure	Lower-directed and localized signal	Higher-passive wide-angle capture

Given this landscape, the lack of a unified methodology for assessing and comparing security risks in OWC systems is evident. Most current approaches rely on qualitative features or isolated experimental results. What remains missing is a structured framework capable of quantifying the likelihood and consequences of threats across technologies. The

RM model, widely used in risk assessment disciplines, provides a compelling solution. By classifying attack vectors based on their severity and frequency, RM enables consistent evaluation of system-level vulnerabilities. In this context, the work of Marin-Garcia et al. [8] applied the RM methodology to VLC, offering a precedent that directly inspires the broader comparative approach adopted in this study for both VLC and OCC.

Taken together, the conceptual analysis in Section 2 and the gaps identified in the related work above highlight the need for a unified, quantitative framework to assess the security posture of VLC and OCC systems. Building on this foundation, the following section details the RM-based methodology used to construct and normalize the comparative risk matrices for both technologies.

4. Methodology

Before describing the technical formulation of the methodology, it is important to clarify that the present work does not apply the RM as a generic management tool. Instead, the RM is extended and adapted to the specific characteristics of optical wireless systems. The methodology used in this study incorporates domain-specific indices, correction factors, and normalization procedures to enable reproducible, technology-aware comparisons between VLC and OCC. These adaptations transform the RM from a descriptive framework into a quantitative instrument capable of capturing feasibility, detectability, channel exposure, and recovery effort—factors that are intrinsic to light-based communication links and not represented in standard ISO/IEC 27005 [10] implementations. At its core, the RM evaluates risk as a function of impact and likelihood, but in this work these dimensions are redefined through optical-channel properties, unified threat modeling, and the proposed Normalized Risk Rank (NRR), which together provide a coherent quantitative basis for cross-technology comparison.

As a concrete illustration of these domain-specific extensions, the "Channel Exposure" correction factor quantifies how optical propagation conditions (LoS, NLoS, and reflective paths) modify the likelihood of successful eavesdropping. This parameter cannot be reproduced using standard ISO/IEC 27005 risk models, and exemplifies the type of OWC-specific adaptations required to make the Risk Matrix applicable to light-based communication systems.

The RM approach was chosen not only for its simplicity and interpretability but also because it aligns with widely recognized international risk management standards, including ISO/IEC 27005 [10] and ISO 31000 [34]. These standards explicitly recommend RM as a systematic and repeatable mechanism for identifying, evaluating, and prioritizing security risks, particularly in emerging or heterogeneous technological environments where extensive quantitative data may not yet exist. In the context of VLC and OCC, where controlled experimentation is costly and sometimes intrusive, RM enables reproducible, transparent vulnerability assessment before deployment. Although any expert-based evaluation inherently involves some degree of subjectivity, this work mitigates it by averaging the independent evaluation of multiple domain specialists, following the procedure described in Section 4.1.

In addition, the RM framework provides a structured, quantifiable way to compare heterogeneous attacks while remaining flexible enough to accommodate the specific characteristics of OWC systems. Unlike purely qualitative assessments, RM enables the translation of expert knowledge and technical indicators into numerical values, which can then be normalized and ranked across scenarios. This approach not only allows the identification of the most critical vulnerabilities in VLC and OCC, but also prioritizes mitigation strategies based on comparable metrics. Furthermore, the methodology aligns with previous research

on network and communication security [35–37], ensuring consistency with established practices while adapting the framework to the specificities of emerging OWC technologies.

From a scientific contribution perspective, this work does not simply reuse the RM as a generic management tool. Building on our previous VLC-only study in [8], we extend and specialize the methodology in four ways that are specific to optical wireless systems. First, we define a unified set of impact and likelihood indices and correction factors that apply consistently to both VLC and OCC, enabling cross-technology comparison on a single quantitative scale. Second, we introduce domain-specific adaptations (feasibility, detectability, channel exposure, and recovery effort) that are absent in generic ISO/IEC 27005 implementations but reflect the physical-layer and architectural properties of light-based communication links. Third, we formalize the Normalized Risk Rank (NRR) as a derived metric that enables heterogeneous attack scenarios and technologies to be compared on a common reference level rather than through ad hoc scoring. Finally, we reconstruct representative attacks (wardriving, DoS, preshared key cracking, and Evil Twin) within a unified, cross-technology threat model, allowing their risk profiles to be evaluated and ranked reproducibly for both VLC and OCC.

4.1. Risk Matrix Methodology

The Risk Matrix is a widely used methodology for risk assessment in engineering and information security. It provides a structured way to evaluate threats across multiple dimensions, including impact, likelihood, severity, and time to recover (TTR). Table 2 summarizes the impact levels, while Table 3 presents the indices considered in the methodology. This work extends our previous study [8], where the methodology was first applied to VLC. Here, we extend the approach to include a systematic comparison between VLC and OCC.

In this work, the numerical values assigned to the different indices do not arise solely from theoretical assumptions. Instead, they are grounded in previous experimental campaigns in which VLC and OCC physical channels were characterized under diverse propagation and obstruction conditions, including line-of-sight and reflected paths, as well as controlled interference scenarios [18–20]. Measured signal levels, error rates, and feasibility of eavesdropping and jamming were first analyzed at the physical layer and then mapped onto the discrete impact and likelihood categories of the RM. This mapping step bridges empirical channel behavior with the qualitative scales used in the risk assessment, ensuring that each evaluated threat reflects realistic operating conditions rather than hypothetical worst-case values.

Table 2 shows the description of impact levels, while Table 3 presents the indices and their corresponding values. These indices are combined using the formulas provided below to calculate the overall Risk Value (RV) associated with each attack.

Table 2. Level description of impact values.

Impact Level	Description
1	Negligible impact
2	Minor impact
3	Moderate impact
4	Major impact
5	Critical impact

Table 3. Indices considered in the Risk Matrix methodology.

Index	Meaning
BP	Business Performance
NL	Network Latency (of target)
IA	Information Access
AD	Attack Duration
TTR	Time to Recover
TD	Technical Difficulty
TK	Technical Knowledge required
ReR	Resource Relation
RA	Required Access

The general risk calculation uses (1) for severity and (2) for Time; both are then applied to (3) to determine the impact.

$$Sev_x = \alpha_1(BP_x) + \alpha_2(NL_x) + \alpha_3(IA_x) \quad (1)$$

$$T_x = \beta_1(AD_x) + \beta_2(TTR_x) \quad (2)$$

$$Impact_x = \eta_1(Sev_x) + \eta_2(T_x) \quad (3)$$

It is important to note that the normalized risk rank (NRR) in this work does not correspond to a strict min–max normalization bounded between 0 and 1. Instead, NRR values are scaled relative to a reference risk level, allowing some scenarios to exceed 1 when their risk rank exceeds the reference. Consequently, values close to 1 indicate risks comparable to the baseline, whereas values above one highlight scenarios with proportionally higher risks.

Table 4 consolidates the correction factors for impact and likelihood. These values are used directly in the above equations without modification.

Table 4. Unified correction factors used in the Risk Matrix (values preserved from the original tables).

Impact Correction Factors							
Factor	α_1	α_2	α_3	β_1	β_2	η_1	η_2
Value	1.05	1.00	1.10	1.05	0.95	1.10	1.00
Likelihood Correction Factors							
Factor	γ_1	γ_2	ϕ_1	ϕ_2	υ_1	υ_2	
Value	1.00	1.00	1.00	1.05	1.05	1.00	

The likelihood (LK_x) was determined by multiple parameters: Technology Difficulty (TD_x), Technology Knowledge (TK_x), Resources Relation (ReR_x), and Required Access to the System (RA_x). These parameters were organized into two intermediate indices: Attack Difficulty ($ADif_x$) and Access to the System (AS_x), as shown below:

$$ADif_x = \gamma_1(TD_x) + \gamma_2(TK_x) \quad (4)$$

$$AS_x = \phi_1(ReR_x) + \phi_2(RA_x) \quad (5)$$

$$LK_x = \upsilon_1(ADif_x) + \upsilon_2(AS_x) \quad (6)$$

Correction factors γ, ϕ, and υ were derived from the expertise of the evaluation group, following the same approach as for impact. Technology difficulty and technology knowledge contributed equally to the $ADif_x$ value ($\gamma_1 = \gamma_2 = 1.00$). For the access index,

the required access (RA) was given more weight than the resource relation (ReR), resulting in a small 5% correction factor. The resulting LK_x values were translated into predefined likelihood levels and correction factors, as summarized in Table 4.

The values assigned to the different attacks were derived from the experience of a group of cybersecurity experts. Each expert independently rated the indices for every attack, and the final values were obtained by averaging their assessments. This approach reduces subjectivity and provides a more reliable estimation of risk levels.

It is also worth noting that differences between VLC and OCC arise in several indices. For example, Time to Recover could be lower in VLC (due to dedicated infrastructure). In contrast, OCC might suffer longer recovery times because of heterogeneous mobile devices if client devices were taken into account. Similarly, detectability could be higher in OCC (artifacts in camera data) than in VLC (invisible to end users), and attack feasibility could be higher in OCC (commodity cameras) than in VLC (requiring access to luminaires). A more detailed discussion of these differences is deferred to Section 5.

The methodology was then applied to four representative attack scenarios: wardriving, evil twin, denial-of-service (DoS) based on the Queensland-alike model, and preshared key attacks. The following Section 4.2 presents the results for each attack, highlighting their differences and impact on VLC and OCC.

4.2. Attacks Scenarios and Risk Evaluation

In order to evaluate the security posture of VLC and OCC, four representative attack scenarios were analyzed: wardriving, evil twin, DoS following the Queensland-alike model, and Preshared Key Cracking (PSK) cracking. Each attack was assessed using the methodology presented in Section 4.1, and the results were consolidated into a unified comparative table. This approach avoids redundancy while retaining the full analytical depth of the original subsections.

Wardriving represents a passive reconnaissance attack in which adversaries attempt to detect and map the presence of VLC or OCC channels by physically moving through the environment. In VLC, the attacker typically relies on photodiodes or light sensors to capture signals from luminaires. In OCC, commodity cameras (e.g., smartphones) can be used, lowering the technical barrier. In the case of OCC, the slowest transmission rate requires longer times to assess the existence and execute the attack properly. Although the overall impact is relatively limited, the attack's feasibility is high, as it requires minimal resources and can be performed covertly. The values in Table 5 confirm that the technical difficulty is slightly higher for OCC due to the need for extra time that makes a cover attack more difficult, while OCC benefits from commodity hardware but remains more detectable. The difference is minimal, but to properly construct the RM and define which areas are more susceptible to attacks or in which scenarios it is better to implement one technology over the other, a single point was introduced in the score.

The Evil Twin (ET) attack consists of deploying a rogue transmitter that impersonates a legitimate source. In VLC, this implies broadcasting signals with modified modulation parameters from an LED luminaire. In OCC, the attack may leverage display-based transmitters or LEDs in consumer electronics. The impact of such an attack is considerable, since it enables traffic interception and manipulation. The risk values indicate higher requirements for technical knowledge (represented by a lower TK value due to the implementation of the methodology equations) compared to OCC, where the attacker must carefully align transmission patterns with camera capture capabilities (represented by a lower RA). In both technologies, however, the feasibility is significant, and the risk levels are elevated.

Queensland DoS attacks in the Queensland-alike model consist of flooding the optical channel with interference, thereby reducing or completely blocking legitimate communi-

cation. In VLC, this can be accomplished by introducing light sources with conflicting frequencies or intensities. In both VLC and OCC, overexposing the sensor with intense light pulses is sufficient to degrade reception. The results highlight that both technologies are vulnerable, and recovery times are similar. The main difference we can see in this attack is the required access level, since there is a smaller area from which to launch it. Overall, this scenario leads to high impact and likelihood levels for both technologies.

Finally, in the case of PSK, the authentication mechanisms may be vulnerable to brute-force or dictionary attacks if they are not sufficiently protected. The same cryptographic suite is applied to VLC. In VLC, cryptographic operations are often implemented at the driver or middleware level. The attack can be simplified when keys are weak or poorly distributed across applications. The results in Table 5 indicate that the technical difficulty is relatively high for both technologies, resulting in a complete compromise of confidentiality and integrity.

Table 5. Risk-matrix indices per attack for VLC and OCC.

Attack	Tech.	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Wardriving	VLC	1	1	2	2	1	5	4	4	5
	OCC	1	1	2	2	1	4	4	4	5
Evil Twin	VLC	3	3	5	5	4	3	4	3	3
	OCC	3	3	5	5	4	2	5	2	2
Queensland-alike DoS	VLC	4	5	1	5	2	4	4	4	4
	OCC	4	5	1	5	2	4	4	4	3
PSK	VLC	3	2	5	5	5	1	1	1	4
	OCC	3	2	5	5	5	1	1	1	4

Note. Expert scores were collected from a panel of three specialists (two academic researchers and one industry engineer) with experience in VLC and OCC systems, following ISO/IEC 27005 risk evaluation scales and the procedure described in Section 4.1.

Note that NRR values may exceed 1, since they are scaled relative to a reference risk level rather than bounded by min–max normalization.

The consolidated outcomes of all four scenarios are shown in Table 5. The table shows that while some indices remain similar across VLC and OCC, there are apparent differences in feasibility, detectability, and recovery time. Wardriving and DoS attacks are more easily performed in OCC environments due to the use of commodity hardware and camera sensitivity, whereas PSK cracking remains a more demanding but highly impactful attack across both technologies.

5. Discussion

Based on the indices and attack scenarios defined in Section 4.2, this section interprets the resulting risk values for VLC and OCC and relates them to the architectural differences discussed in Section 2. The unified risk evaluation, summarized in Table 5 and quantified using the Risk Rank (RR) and Normalized Risk Rank (NRR) formulations in (7) and (8), reveals consistent yet technology-specific security patterns for VLC and OCC. These findings align with prior surveys and empirical studies [8,38,39], but extend them by quantifying risk values instead of relying solely on qualitative assessments. Unlike earlier works that highlighted vulnerabilities descriptively, our structured RM analysis provides a measurable comparison that enables systematic evaluation across scenarios.

$$RR_x = \varrho_1 \cdot Impact_x \cdot \frac{LK_x}{\varrho_2} \tag{7}$$

$$NRR_x = \frac{RR_x \cdot E}{\sum\limits_{i \in E} RR_i}; \quad x \in E \tag{8}$$

As illustrated in Figure 1, architectural differences significantly shape the threat landscape. VLC, designed for continuous modulation and integration with network stacks, exposes a broader attack surface for interception and traffic manipulation. OCC, constrained by camera frame capture and processing pipelines, is inherently less attractive for large-scale eavesdropping but more vulnerable to resource exhaustion and denial-of-service. The distribution of evaluated scenarios in the risk space (Figure 2) further substantiates these tendencies: clusters associated with interception and traffic manipulation concentrate toward higher perceived impact under VLC, whereas availability-driven conditions align with OCC's camera-centric bottlenecks. This visualization provides an empirical cross-check against the ranked outcomes in Tables 5 and 6.

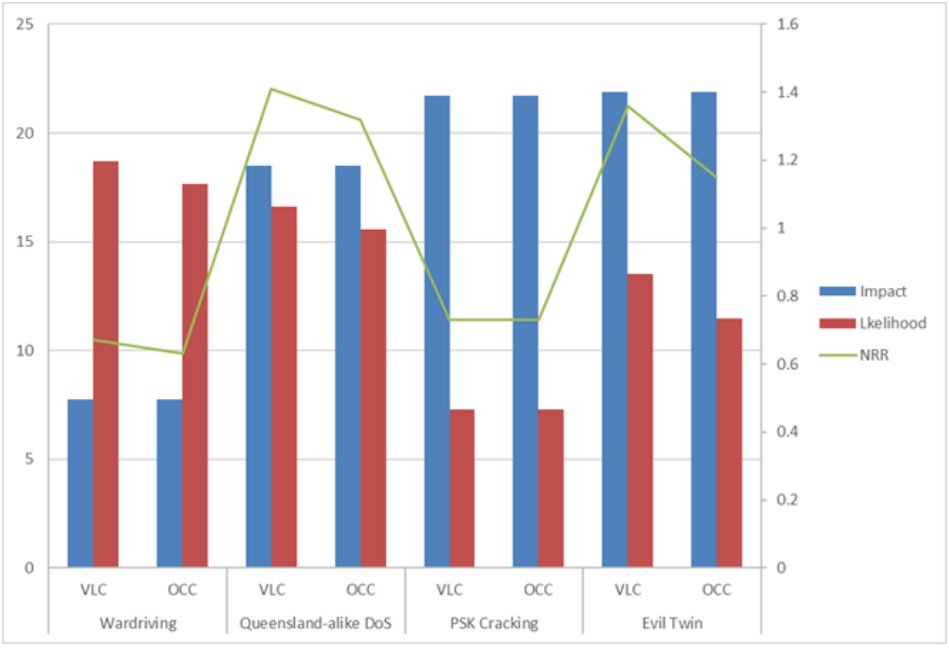

Figure 2. Comparative representation of the evaluated attack scenarios. The left axis depicts the values of Impact and Likelihood, while the right axis shows the corresponding Normalized Risk Rank (NRR) (green line). This combined view highlights the relationship between impact, occurrence probability, and the resulting normalized risk across different attacks.

As detailed in the methodology, the values were derived from expert judgment and averaged. This context is essential to interpret the relative positioning of the scenarios in Table 6 and Figure 2. Furthermore, the RM methodology provides a structured framework for analyzing differences in risk across multiple technologies and identifying areas of higher exposure where resources should be prioritized, as described in [8].

In parallel with risk-oriented analyses, the physical-layer community has begun exploring intelligent metasurface architectures to enhance intensity detection and channel robustness in optical and RF–optical hybrid links. Liu et al. [40] present a comprehensive overview of stacked intelligent metasurfaces for wireless communications, emphasizing how reconfigurable electromagnetic structures can enhance energy focusing, encoding flexibility, and resilience against channel impairments. Although their work is not specific to VLC or OCC, the underlying idea of controllable spatial and intensity shaping is directly compatible with the mitigation strategies discussed in this paper, particularly for reducing the feasibility and impact of jamming and interception attacks in light-based wireless systems.

The indices in Table 5 reflect a slight but meaningful asymmetry: technical difficulty is lower for OCC (TD: 4) than for VLC (TD: 5), consistent with the availability of commodity cameras; both technologies present identical values for required access ($RA = 5$) and

reconnaissance feasibility. While OCC may require longer dwell times due to frame-based throughput, the barrier to entry remains low. Overall, wardriving remains a low-impact, high-feasibility reconnaissance vector for both stacks, which justifies its position in the low-impact/high-likelihood region of the risk space.

For ET, the table shows a mixed profile: OCC exhibits a lower technical difficulty (TD: 2 vs. 3 in VLC) and a lower required access (RA: 2 vs. 3), but a higher technical knowledge requirement (TK: 5 vs. 4), reflecting the need to align transmission patterns with camera sampling and exposure. In practice, both technologies face elevated risk because impersonation enables traffic manipulation and session hijacking. The differences captured by TD/TK/RA explain the relative positions and support the conclusion that ET remains a priority threat in deployments with weak authentication binding.

The indices converge across stacks (TD: 4, TTR: 2), with OCC requiring even less access (RA: 3 vs. 4 in VLC), which broadens the attacker's operational envelope. Since both systems can be degraded by overexposure or conflicting light patterns, the scenario naturally maps to high-likelihood/high-impact regions. Because recovery (TTR) is not negligible and mitigation may involve camera reinitialization or application-layer resets, the availability risk is particularly acute for OCC.

The table confirms that technical difficulty and technical knowledge are low and equal across stacks (TD: 1, TK: 1), with comparable access preconditions (RA: 4). However, the potential impact is higher in VLC (Impact: 5 vs. 4 in OCC), since compromise of PSK directly undermines confidentiality and integrity in higher-throughput channels. These values justify higher RR/NRR for VLC in authentication-driven scenarios and emphasize the need for robust key management.

The detailed scores reported in Table 6 are consistent with the index-level shifts above: eavesdropping and traffic injection reach higher criticality in VLC, driven by broadcast illumination and higher data rates, which increase adversarial payoff with commodity photodiodes [8]. In contrast, OCC interception typically yields lower-value data due to frame constraints, yet denial-of-service conditions are easier to trigger and harder to absorb, as suggested by the lower RA and non-negligible TTR values.

Table 6. Risk Rank (RR) and Normalized Risk Rank (NRR) computed from the indices in Table 5 using Equations (7) and (8). Correction factors per Table 4. Here, $\varrho_1 = \varrho_2 = 1.00$.

Attack	Tech	$Impact_x$	LK_x	ϱ_1	ϱ_2	RR	NRR
Wardriving	VLC	7.73	18.70	1.00	1.00	144.46	0.67
	OCC	7.73	17.65	1.00	1.00	136.35	0.63
Queensland-alike DoS	VLC	18.48	16.60	1.00	1.00	306.77	1.41
	OCC	18.48	15.55	1.00	1.00	287.36	1.32
PSK Cracking	VLC	21.72	7.30	1.00	1.00	158.52	0.73
	OCC	21.72	7.30	1.00	1.00	158.52	0.73
Evil Twin	VLC	21.87	13.50	1.00	1.00	295.18	1.36
	OCC	21.87	11.45	1.00	1.00	250.35	1.15

Table 4 clarifies how feasibility, detectability, and recovery time shape practical risk. VLC attacks are comparatively easy to mount with off-the-shelf components and often remain unnoticed (lighting fluctuations), whereas OCC attacks require more specialized tuning (higher TK in some scenarios) but tend to produce visible artifacts or latency, improving detection at the cost of longer recovery. The resulting trade-off is that OCC's relative resistance to large-scale interception comes with reduced resilience to adversarial load.

From a deployment perspective, these findings carry concrete implications. VLC is ill-suited to environments where confidentiality is paramount (e.g., vehicular networks, smart offices, industrial automation) unless complemented by robust cryptography, channel

randomization, and active intrusion detection. Conversely, OCC should be avoided in latency-sensitive or safety-critical applications, since its susceptibility to denial-of-service and longer recovery paths can undermine operational resilience. These results nuance the related work by making the trade-offs explicit and measurable via RR/NRR, offering system designers an actionable framework rather than general qualitative guidance.

Finally, taken together, the ranked metrics (RR/NRR) and the spatial distribution in Figure 2 yield a coherent picture: VLC concentrates confidentiality-driven risks, while OCC concentrates availability-driven risks under adversarial load. The security posture of each stack is thus determined not only by the feasibility of attacks but also by the operational context and recovery dynamics. This critical perspective bridges the gap between the methodology and empirical results, motivating the recommendations presented in Section 6.

6. Conclusions

This work revisited the comparative security posture of VLC and OCC using a structured RM methodology and the set of indices in Table 5. By quantifying attack scenarios through the Risk Rank (RR) and Normalized Risk Rank (NRR) metrics in Equations (7) and (8), and by applying the unified correction factors in Table 4, we provide a reproducible, data-driven basis for technology selection.

It should be acknowledged that the present analysis was conducted under specific simplifying assumptions regarding the system architecture. In particular, we modeled a cell-based deployment in which each luminaire operates as an independent access point. This choice reflects the most common and practical approach for both VLC and OCC, as it directly leverages existing illumination infrastructure and minimizes the need for specialized hardware or complex coordination mechanisms. However, this assumption naturally constrains the scope of our conclusions. Alternative configurations, such as cell-free or distributed Multiple Input Multiple Output (MIMO) architectures [41], where multiple luminaires jointly serve users, or the use of advanced optical front-ends such as beam-steering, adaptive optics, or stacked intelligent metasurface architectures [40,42] would likely change the assessed risk profile. By introducing spatial diversity, redundancy, and targeted energy delivery, these more sophisticated designs could significantly reduce the feasibility and impact of several critical threats. For example, Queensland-like denial-of-service attacks would face higher barriers due to spatial multiplexing and coordinated resource management. At the same time, the effectiveness of Evil Twin impersonation would be limited by dynamic beam alignment and user-luminaire binding. In such scenarios, both the likelihood and impact scores underpinning our risk estimates would shift downward, lowering the overall risk rank associated with these attacks. Nevertheless, it is essential to emphasize that the majority of current and foreseeable VLC/OCC deployments, particularly in indoor networking and infrastructure-based contexts, are expected to adopt the simpler cell-based model for reasons of cost, compatibility, and ease of integration with lighting systems. Accordingly, while our analysis does not exhaustively capture the spectrum of possible architectures, it can be considered representative of the most prevalent and realistic deployment environments, and thus provides a valid and broadly applicable basis for comparing the security posture of the two technologies.

The results confirm a clear separation of dominant risks. VLC concentrates confidentiality-driven exposure: interception and traffic manipulation remain more critical under broadcast illumination and higher data rates, and the scores place Evil Twin and PSK scenarios among the top risk contributors for VLC. At the same time, availability-driven stress is prominent across both stacks under Queensland-alike DoS, with VLC exhibiting the highest RR/NRR overall due to the combination of elevated impact and likelihood. For OCC, the values corroborate lower payoff for bulk interception but heightened sensitivity

to adversarial load, consistent with camera-centric bottlenecks observed in the risk-space clustering (Figure 2).

Index-level asymmetries explain these outcomes. In the table, Wardriving maintains low impact yet high feasibility for both technologies, with slightly lower technical difficulty for OCC (TD: 4 vs. 5) reflecting commodity cameras. For Evil Twin, OCC shows reduced required access (RA: 2 vs. 3) but higher technical knowledge (TK: 5 vs. 4), mirroring alignment constraints with frame sampling. Under Queensland-alike DoS, access prerequisites are looser for OCC (RA: 3 vs. 4), which broadens the attacker's operational envelope and helps explain its availability risks despite comparable impact. These fine-grained differences propagate through the RR/NRR pipeline and are visible in the scenario clusters.

From a deployment standpoint, the updated evidence supports concrete guidance. VLC should not be chosen where confidentiality is paramount (e.g., vehicular networks, smart offices, industrial automation) unless reinforced with strong cryptography, robust authentication (binding against ET), channel randomization, and active intrusion detection. On the other hand, OCC is unsuitable for latency-sensitive or safety-critical control, where denial-of-service and a possible longer recovery paths (*TTR*) can undermine operational resilience; rate-limiting at the vision pipeline, adaptive exposure control, and fail-safe handover policies are recommended mitigations. In mixed environments, designers should explicitly trade confidentiality against availability using RR/NRR as a decision aid rather than relying on throughput or convenience alone.

Methodologically, the updated analysis highlights the value of combining RR/NRR with expert-elicited correction factors, as it converts qualitative insights into testable and reproducible statements, facilitating comparison across technologies and contexts. The alignment between ranked outcomes (Table 6) and spatial distribution in Figure 2 provides an internal consistency check that strengthens the conclusions.

Author Contributions: Conceptualization, I.M.-G. and V.G.; methodology, I.M.-G.; software, I.M.-G.; validation, I.M.-G., V.G. and R.P.-J.; formal analysis, I.M.-G.; investigation, I.M.-G.; resources, I.M.-G.; data curation, V.G.; writing—original draft preparation, I.M.-G.; writing—review and editing, V.G., J.R. and R.P.-J.; visualization, I.M.-G.; supervision, R.P.-J. and J.R.; project administration, I.M.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Spanish Ministry of Research, Universities and Innovation, under the grant PID2024-155330OB-C21 (Project VELOCITY).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Conflicts of Interest: Victor Guerra was employed by the company Wooptix S.L. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AD	Attack Duration
ADif	Attack Difficulty
AS	Access to the System
BP	Business Performance
CDMA	Code Division Multiple Access
CMOS	Complementary Metal–Oxide–Semiconductor
COMSEC	Communication Security
CSK	Color Shift Keying
DoS	Denial of Service

ET	Evil Twin
FoV	Field-of-View
IA	Information Access
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ITU	International Telecommunication Union
LED	Light Emitting Diode
Li-Fi	Light Fidelity
LoS	Line-of-Sight
LK	Likelihood
MIMO	Multiple Input Multiple Output
NATO	North Atlantic Treaty Organization
NFC	Near-Field Communication
NLoS	No-Line-of-Sight
NRR	Normalized Risk Rank
OCC	Optical Camera Communication
OFDM	Orthogonal Frequency-Division Multiplexing
OOK	On-Off Keying
OWC	Optical Wireless Communication
PHY	Physical Layer
PPM	Pulse Position Modulation
PSF	Point Spread Function
PSK	Preshared Key Cracking
RA	Required Access to System
ReR	Resource Relation
RF	Radio Frequency
RIS	Reconfigurable Intelligent Surface
RM	Risk Matrix
RGB	Red–Green–Blue
ROI	Region of Interest
RR	Risk Rank
Sev	Severity
SNR	Signal-to-Noise Ratio
TD	Technology Difficulty
TK	Technical Knowledge
TTR	Time to Recover
USA	United States of America
VLC	Visible Light Communication
WD	Wardriving
WLAN	Wireless Local Area Network

Appendix A. Supplementary Technical Parameters

This appendix consolidates descriptive and implementation-specific details that support the comparative analysis of VLC and OCC systems presented in Section 2. These aspects were moved here to streamline the main discussion and emphasize the article's security-oriented perspective.

Appendix A.1. VLC Physical-Layer Parameters

Visible Light Communication (VLC) systems rely on intensity-modulated light emitted by LED sources, typically operating between 380 nm and 750 nm. Common modulation formats include On-Off Keying (OOK), Pulse Position Modulation (PPM), Color Shift Keying (CSK), and Orthogonal Frequency-Division Multiplexing (OFDM). Each format represents a trade-off between spectral efficiency, flicker mitigation, and receiver complexity. Typical

laboratory demonstrations achieve data rates from a few Mbps up to several Gbps, depending on the LED package, driving electronics, and optical front-end bandwidth. The modulation bandwidth is often limited by parasitic capacitances in series-connected LED arrays, which may require partial decoupling or pre-equalization networks to reach high-speed operation.

Appendix A.2. Optical Channel and Receiver Characteristics

The optical wireless channel in VLC is affected by direct line-of-sight and reflected components. The received optical power, P_r, depends on the LED radiant intensity, the photodiode responsivity, and the geometry of the transmitter–receiver pair. Ambient illumination and fluorescent flicker introduce additional shot noise, potentially reducing the effective SNR. Commercial photodiodes with transimpedance amplifiers typically exhibit responsivities between 0.2 and 0.6 A/W and are equipped with optical filters to reject sunlight and infrared interference.

Appendix A.3. OCC Camera Parameters

Optical Camera Communication (OCC) systems employ CMOS image sensors that capture modulated light within successive frames. Cameras may use rolling-shutter or global-shutter acquisition: the former allows high effective symbol rates through line-by-line exposure, while the latter provides uniform frame integration at the cost of bandwidth. Data reconstruction accuracy depends on exposure time, lens aperture, focal length, and frameof 0.2–30–240 fps for consumer cameras). Motion blur, ambient light saturation, and automatic-gain algorithms can significantly distort the optical waveform; these factors must be modeled when estimating achievable throughput and reliability.

Appendix A.4. OCC Physical-Layer and Modulation Parameters

In OCC, data is embedded into visual signals using techniques that vary in complexity and channel assumptions:

- Rolling shutter exploitation: Many CMOS sensors acquire frames line-by-line, allowing high-speed modulation to be reconstructed from stripe patterns. This enables frame-level throughput improvements without increasing the frame rate.
- Spatiotemporal coding: Data can be encoded across pixels and frames, using M-PAM, Manchester coding, or color-based modulation (e.g., Red–Green–Blue (RGB) flickering, chromatic encoding).
- Multiple transmitters per frame: OCC cameras can decode data from dozens of emitters simultaneously, enabling scalable many-to-one communication and localization.
- Image-aware channel modeling: System performance depends on depth-of-field, focal length, and sensor response, which are now being modeled using camera optics and Point Spread Function (PSF).
- Emerging topics: Research has explored sub-pixel encoding, where emitters are detected and decoded even when projected to areas smaller than a pixel, and OCC-based positioning through LED visual beacons.

Appendix A.5. Hybrid and Emerging Schemes

Recent works explore spatiotemporal coding, sub-pixel encoding, and multi-LED spatial multiplexing to increase the aggregate capacity of optical links. Hybrid VLC/OCC configurations combine high-speed photodiodes for uplink transmission with camera receivers for downlink or localization tasks, leveraging the complementary strengths of both modalities. Such architectures illustrate how physical-layer diversity can enhance availability and resilience—concepts that directly inform the risk-assessment framework adopted in this paper.

These detailed parameters are not central to the qualitative risk comparison but are included here for completeness and reproducibility.

References

1. Souppaya, M.; Scarfone, K. Guidelines for Securing Wireless Local Area Networks (WLANs). *NIST Spec. Publ.* **2012**, *800*, 153. [CrossRef]
2. Lutovac, V.; Kočan, E. Physical Layer Security in Wireless Networks—Concept, Performance and Perspectives. In Proceedings of the 2025 29th International Conference on Information Technology (IT), Žabljak, Montenegro 19–22 February 2025. [CrossRef]
3. Zhang, X.; Klevering, G.; Lei, X.; Hu, Y.; Xiao, L.; Tu, G.H. The Security in Optical Wireless Communication: A Survey. *ACM Comput. Surv.* **2023**, *55*, 1–36. [CrossRef]
4. Liu, X.; Wang, W.; Song, G.; Zhu, T. LightThief: Your Optical Communication Information is Stolen behind the Wall. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 5325–5339, ISBN 978-1-939133-37-3.
5. Riurean, S.; Dobre, R.A.; Marcu, A.E. Security and propagation issues and challenges in VLC and OCC systems. In *Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X*; Vladescu, M., Tamas, R.D., Cristea, I., Eds.; International Society for Optics and Photonics, SPIE: Bellingham, WA, USA, 2020; Volume 11718, p. 117182B. [CrossRef]
6. Ximenes, L.; de Almeida Larêdo, B. A Tensor-Based Optical Camera Communication (OCC) System with Joint Data Detection and Video Restoration. *Authorea* **2023**, *preprint*. [CrossRef]
7. Khan, M.A.; Menouar, H.; Nassar, A.; Abdallah, M. Visual Deception: Demonstrating Spoofing Attacks on Autonomous Vehicle Cameras. In Proceedings of the 2024 International Conference on Future Technologies for Smart Society (ICFTSS), Kuala Lumpur, Malaysia, 7–8 August 2024; pp. 165–168. [CrossRef]
8. Marín-García, I. Considerations on Visible Light Communication Security by Applying the Risk Matrix Methodology for Risk Assessment. *PLoS ONE* **2017**, *12*, e0188759. [CrossRef] [PubMed]
9. U.S. Department of Homeland Security. *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*; Technical Report; U.S. Department of Homeland Security: Washington, DC, USA, 2011.
10. *ISO/IEC 27005:2022*; Information Security, Cybersecurity and Privacy Protection—Guidance on Information Security Risk Management. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/80585.html (accessed on 30 November 2025).
11. Vautherin, J.; Rutishauser, S.; Schneider-Zapp, K.; Choi, H.F.; Chovancova, V.; Glass, A.; Strecha, C. Photogrammetric Accuracy and Modeling of Rolling Shutter Cameras. *Isprs Ann. Photogramm. Remote. Sens. Spat. Inf. Sci.* **2016**, *III-3*, 139–146. [CrossRef]
12. Xu, J.; Li, F.; Han, L.; Gao, Z.; Wang, H. Analysis of signal attenuation in global shutter CMOS image sensor. *Microelectron. Reliab.* **2020**, *109*, 113678. [CrossRef]
13. Matus, V.; Guerra, V.; Jurado-Verdu, C.; Rabadan, J.; Perez-Jimenez, R. Demonstration of a Sub-Pixel Outdoor Optical Camera Communication Link. *IEEE Lat. Am. Trans.* **2021**, *19*, 1798–1805. [CrossRef]
14. Younus, O.I.; Bani Hassan, N.; Ghassemlooy, Z.; Haigh, P.A.; Zvanovec, S.; Alves, L.N.; Minh, H.L. Data Rate Enhancement in Optical Camera Communications Using an Artificial Neural Network Equaliser. *IEEE Access* **2020**, *8*, 42656–42665. [CrossRef]
15. Zhang, P.; Liu, Z.; Hu, X.; Sun, Y.; Deng, X.; Zhu, B.; Yang, Y. Constraints and Recent Solutions of Optical Camera Communication for Practical Applications. *Photonics* **2023**, *10*, 608. [CrossRef]
16. Kolade, O.; Cox, M.A.; Cheng, L. Visible light communication using a software-defined radio approach. In *Fifth Conference on Sensors, MEMS, and Electro-Optic Systems*; du Plessis, M., Ed.; International Society for Optics and Photonics, SPIE: Bellingham, WA, USA, 2019; Volume 11043, p. 110430Z. [CrossRef]
17. Huang, S.; Dehghani Soltani, M.; Safari, M. Physical-Layer Security for Optical Wireless Communications. In *Physical-Layer Security for 6G*; Bloch, M., Ed.; Wiley: Hoboken, NJ, USA, 2024; pp. 67–97. [CrossRef]
18. Marín-García, I.; Guerra, V.; Pérez-Jiménez, R. Study and Validation of Eavesdropping Scenarios over a Visible Light Communication Channel. *Sensors* **2017**, *17*, 2687. [CrossRef]
19. Cui, M.; Feng, Y.; Wang, Q.; Xiong, J. Sniffing visible light communication through walls. In Proceedings of the MobiCom '20: 26th Annual International Conference on Mobile Computing and Networking, London, UK, 21–25 September 2020. [CrossRef]
20. Marin-Garcia, I.; Chavez-Burbano, P.; Muñoz-Arcentles, A.; Calero-Bravo, V.; Perez-Jimenez, R. Indoor location technique based on visible light communications and ultrasound emitters. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 9–12 January 2015; pp. 297–298. [CrossRef]
21. Arfaoui, M.A.; Soltani, M.D.; Tavakkolnia, I.; Ghrayeb, A.; Safari, M.; Assi, C.M.; Haas, H. Physical Layer Security for Visible Light Communication Systems: A Survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1887–1908. [CrossRef]
22. Su, N.; Panayirci, E.; Koca, M.; Yesilkaya, A.; Poor, H.V.; Haas, H. Physical Layer Security for Multi-User MIMO Visible Light Communication Systems With Generalized Space Shift Keying. *IEEE Trans. Commun.* **2021**, *69*, 2585–2598. [CrossRef]
23. Saeed, N.; Guo, S.; Park, K.H.; Al-Naffouri, T.Y.; Alouini, M.S. Optical camera communications: Survey, use cases, challenges, and future trends. *Phys. Commun.* **2019**, *37*, 100900. [CrossRef]
24. Zhang, X.; Liu, J.; Ba, Z.; Tao, Y.; Cheng, X. MobiScan: An enhanced invisible screen-camera communication system for IoT applications. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4151. [CrossRef]

25. Figueiredo, G.; André, P.S.; Ferreira, R.A.S. Security Enhanced Encryption on Color Modulation of Visible Light Communication Systems. In Proceedings of the 2023 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC), Castelldefels, Spain, 5–9 November 2023; pp. 268–270. [CrossRef]
26. Iqbal, R.; Biagi, M.; Zoha, A.; Imran, M.A.; Abumarshoud, H. Leveraging IRS Induced Time Delay for Enhanced Physical Layer Security in VLC Systems. *arXiv* **2024**, arXiv:2402.03202. [CrossRef]
27. Abumarshoud, H.; Chen, C.; Tavakkolnia, I.; Haas, H.; Imran, M.A. Intelligent Reflecting Surfaces for Enhanced Physical Layer Security in NOMA VLC Systems. In Proceedings of the IEEE International Conference on Communications (ICC), Rome, Italy, 28 May–1 June 2023. [CrossRef]
28. Soderi, S.; Brighente, A.; Xu, S.; Conti, M. VLC Physical Layer Security through RIS-aided Jamming Receiver for 6G Wireless Networks. In Proceedings of the IEEE SECON 2022, Virtual, 20–23 September 2022; pp. 370–378. [CrossRef]
29. Nguyen, D.T.; Park, S.; Chae, Y.; Park, Y. VLC/OCC hybrid optical wireless systems for versatile indoor applications. *IEEE Access* **2019**, *7*, 22371–22376. [CrossRef]
30. Abuella, H.; Elamassie, M.; Uysal, M.; Xu, Z.; Serpedin, E.; Qaraqe, K.A.; Ekin, S. Hybrid RF/VLC Systems: A Comprehensive Survey on Network Topologies, Performance Analyses, Applications, and Future Directions. *IEEE Access* **2021**, *9*, 160402–160436. [CrossRef]
31. Kazik, T.; Nguyen, T.H.; Rahaim, M.B.; Little, T.D.C. Optical Camera Communication: Perspectives and Challenges. In Proceedings of the IEEE Photonics Conference (IPC), San Diego, CA, USA, 12–16 October 2014; pp. 505–506. [CrossRef]
32. Marin-Garcia, I.; Ramirez-Aguilera, A.M.; Guerra, V.; Rabadan, J.; Perez-Jimenez, R. Data sniffing over an open VLC channel. In Proceedings of the 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Prague, Czech Republic, 20–22 July 2016; pp. 1–6. [CrossRef]
33. Matheus, L.E.M.; Vieira, A.B.; Vieira, L.F.M.; Vieira, M.A.M.; Gnawali, O. Visible Light Communication: Concepts, Applications and Challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 3204–3237. [CrossRef]
34. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 30 November 2025).
35. Fu, S.; Zhou, H.; Xiao, Y. The application of a risk matrix method on campus network system risk assessment. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011; pp. 474–478. [CrossRef]
36. Xiaosong, L.; Shushi, L.; Wenjun, C.; Songjiang, F. The Application of Risk Matrix to Software Project Risk Management. In Proceedings of the 2009 International Forum on Information Technology and Applications, Chengdu, China, 15–17 May 2009; Volume 2, pp. 480–483. [CrossRef]
37. Li, Z.P.; Yee, Q.M.G.; Tan, P.S.; Lee, S. An extended risk matrix approach for supply chain risk assessment. In Proceedings of the 2013 IEEE International Conference on Industrial Engineering and Engineering Management, Bangkok, Thailand, 10–13 December 2013; pp. 1699–1704. [CrossRef]
38. Burchardt, H.; Serafimovski, N.; Tsonev, D.; Videv, S.; Haas, H. VLC: Beyond Point-to-Point Communication. *IEEE Commun. Mag.* **2014**, *52*, 98–105. [CrossRef]
39. Haas, H.; Yin, L.; Wang, Y.; Chen, C. What is LiFi? *J. Light. Technol.* **2016**, *34*, 1533–1544. [CrossRef]
40. Liu, H.; An, J.; Jia, X.; Gan, L.; Karagiannidis, G.K.; Clerckx, B.; Bennis, M.; Debbah, M.; Cui, T.J. Stacked Intelligent Metasurfaces for Wireless Communications: Applications and Challenges. *IEEE Wirel. Commun.* **2025**, *32*, 46–53. [CrossRef]
41. Beysens, J.; Wang, Q.; Galisteo, A.; Giustiniano, D.; Pollin, S. A Cell-Free Networking System With Visible Light. *IEEE/ACM Trans. Netw.* **2020**, *28*, 461–476. [CrossRef]
42. Jian, Y.H.; Wang, C.C.; Chow, C.W.; Gunawan, W.H.; Wei, T.C.; Liu, Y.; Yeh, C.H. Optical Beam Steerable Orthogonal Frequency Division Multiplexing1 (OFDM) Non-Orthogonal Multiple Access (NOMA) Visible Light Communication Using Spatial-Light Modulator Based Reconfigurable Intelligent Surface. *IEEE Photonics J.* **2023**, *15*, 7303408. [CrossRef]