

# Abstract

for Poster Presentation

**Title:** A Structural Steganographic Framework for Confidential Data Transmission in LiFi Networks

**Authors:** Ramin Irani, Siamak Khatibi.

*Light Fidelity presents a high-speed and interference-resilient alternative to traditional wireless communication technologies, making it particularly suitable for sensitive domains such as healthcare, defense, and industrial control systems. Although LiFi inherently benefits from line-of-sight transmission, which offers an additional layer of physical security, it remains vulnerable to localized eavesdropping and insider interception within the communication range. These vulnerabilities highlight the necessity for supplementary data-centric security mechanisms that are compatible with the operational characteristics and resource constraints of LiFi environments.*

*This research introduces a novel steganographic framework specifically designed for matrix-structured data, a format widely utilized across digital communication and sensing systems. To validate the effectiveness of the proposed method, digital images—naturally represented as two-dimensional matrices—are employed as experimental datasets. Unlike conventional steganographic approaches that rely on payload embedding and are therefore susceptible to statistical detection, the proposed technique transforms the intrinsic structure of the data itself through recursive segmentation, matrix reshaping, and hierarchical tree-based indexing.*

*The proposed transformation process generates encrypted outputs that exhibit noise-like statistical properties, thereby concealing both the underlying information and the existence of hidden communication. Experimental analysis using quantitative metrics, including entropy, correlation coefficients, contrast, homogeneity, and Bhattacharyya Distance, demonstrates that the encrypted matrices achieve substantial statistical obfuscation while still enabling lossless reconstruction of the original data through inverse recursive operations.*

*Furthermore, the lightweight computational design of the framework makes it suitable for deployment in resource-constrained LiFi-enabled sensor nodes and embedded systems. By restructuring data at the matrix level rather than embedding information within an existing carrier, the proposed approach establishes a robust and generalizable security framework for confidential communication in physically exposed yet high-bandwidth LiFi networks.*