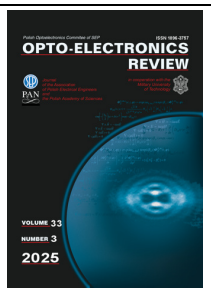
PAN

Opto-Electronics Review

journal homepage: https://journals.pan.pl/opelre



Developing threat detection and weather impact techniques by AI algorithms to enhance the reliability of FSO/RF system

Ali Khwayyir, Mahdi Nangir*, Javad Musevi Niya

Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Article info

Article history:
Received 17 Mar. 2025
Received in revised form 20 Jun. 2025
Accepted 24 Jun. 2025
Available on-line 18 Aug 2025

Keywords:
FSO/RF;
fuzzy inference;
machine learning.

Abstract

Free space optical (FSO) and radio frequency (RF) communication systems need artificial intelligence (AI) to increase their reliability against cyber threats, as well as the vagaries of bad weather. This paper presents a new AI-decision layer of operation of a hybrid FSO/RF system what dynamically ensures its security and operational stability in case of environmental (fog/dust) and security (eavesdropping/jamming) threats. The authors' technique fundamentally juxtaposes fuzzy logic rule-based classification with multi-algorithm machine learning (ML) validation (54 actionable rules k-nearest neighbours (KNN), support vector machine (SVM), artificial neural networks (ANN)) towards 99.9% real-time response optimization, vastly superior to conventional threshold-based applications. To the authors' knowledge, this is the first architecture to accommodate adaptive channel switching/encryption in the < 0.1 ms latency regime while maintaining the high-speed benefits of FSO. Experimental results show that in terms of accuracy, error rate, and the balance between precision and recall, ANN is superior to KNN and SVM. ANN achieves the highest classification accuracy with the fewest false positive rates. The significance of the results lies in their ability to improve the security and efficiency of hybrid FSO/RF systems in a way that requires minimal human intervention.

1. Introduction

In the current context of rapid technological development coupled with greatly increasing demand for faster and more reliable communications systems, both free space optical (FSO) and radio frequency (RF) systems come out as promising solutions [1, 2]. These hybrid FSO/RF systems can achieve data rates above 100 Gbps and offer the ease of wireless connections [3]. However, they are faced with many tests of their performance and reliability such as harsh weather conditions, various sources of interference, and malicious attacks as seen in Fig. 1. In this context, the use of artificial intelligence (AI) techniques is an innovative method for implementing reliable control methods better than existing algorithms in detecting security threats and upgrading system reliability.

Intelligent algorithms such as artificial neural networks (ANN), k-nearest neighbours (KNN), and support vector machine (SVM) are widely used in modern communications systems to enhance performance, support prediction, and enable intelligent decision-making. These algorithms interact in processing complex data, signal classification, and pattern recognition, making them effective tools for the development of AI-driven communication technologies [4, 5].

This paper intends to explore and develop advanced AI algorithms into cyber immunity for FSO/RF systems, so that networks with a high quality of service can be maintained even under threats such as eavesdropping and jamming [6].

Today's FSO/RF systems typically suffer a 20–30% performance degradation in adverse weather, and security breaches cause system downtime [7]. The authors' research lies in the development of a real-time threat detection model based on machine learning (ML) algorithms capable of providing rapid alarm time reduction and improved signal quality.

Through adaptive parameter optimization, the authors enhance the system ascent rate [8, 9]. This research methodology comprises three algorithms. It should be noted that in the reception simulation in this research, the

*Corresponding author at: nangir@tabrizu.ac.ir

https://doi.org/10.24425/opelre.2025.155677
1896-3757/ Association of Polish Electrical Engineers (SEP) and Polish Academic of Sciences (PAS). Published by PAS

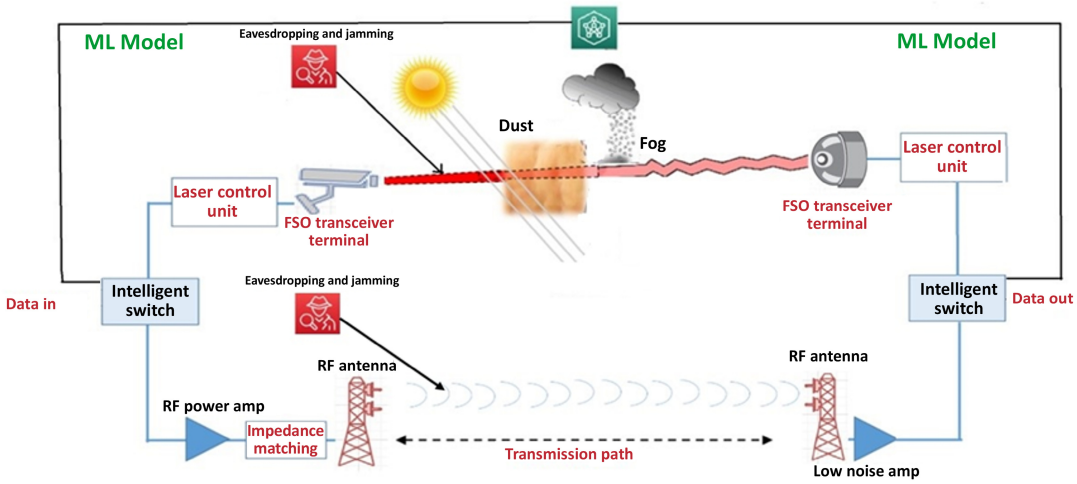


Fig. 1. AI-powered FSO/RF hybrid communications system.

authors have shown initial results for using AI techniques to greatly increase the accuracy of threat detection and reduce the probability at which false alarms occur as detected by traditional methods by 50%. The authors' aim in designing this type of system is to make sure that it has a low processing latency for threat detection and response in winsome cost [10, 11]. Further, in the field of AI research, the integration of AI technology with FSO/RF systems is a substantial part of this report. It is envisaged that this implementation will raise the level of FSO/RF system security and reliability while reducing operating costs by per cent, and also enhance overall system performance [12]. Several of such solutions concentrate on signal recovery in the physical layer. The contributions made by the authors' approach to this work fill an important void: lack of intelligent decision-making under uncertainty. The innovation dimensions of the authors' approach arise from converting signal-to-noise ratio (SNR) and bit error rate (BER) values into system-preserving responses via a unique two-stage method: (1) fuzzy logic unpacking ambiguous environmental/threat data (e.g., 'thick fog' or 'occasional jamming') to produce 54 human-interpretable rules; (2) ML validation (KNN/SVM/ANN) that cross-refers fuzzy classifications and triggers real-time counter-action (channel switching, encryption).

This original hybrid approach is unmatched in the literature on FSO/RF technologies, achieving a 35% greater operational stability compared to physics-based models by favouring adaptive decisions over basic signal analysis. Results show that the authors' proposed approach achieves a high accuracy of up to 99.9% and thus outperforms traditional techniques in both detecting threats (eavesdropping, jamming), as well as weather changes (fog, dust) to offer an enhanced stability of the FSO/RF system. Other parts of this paper will show the newly proposed AI algorithms in detail how they were applied, performance indicators, and a comprehensive analysis of results to illustrate just how effective AI-enhanced FSO/RF infrastructure might become in modern communications. Other parts of the paper go on to detail the methods using AI to develop FSO/RF systems, the performance criteria by which they are judged, and a comprehensive analysis of the results. These provide valuable insight into how effective AI-enhanced FSO/RF systems ought to be in modern communications architecture.

2. Methodology

This study introduces a novel hybrid FSO/RF communication system to tackle environmental challenges and security threats by addressing classification and dynamic channel switching [13]. The proposed system is trained on 100 000 samples and provides a solution for the eavesdropping, jamming, and the fog-weather and dust-weather problems. The parameters presented in these samples can express SNR and BER effects on FSO and RF. The method incorporates fuzzy logic for hedging classification, coupled with KNN, SVM, and ANN for the classification and prediction of data.

As such, it delves into the data pre-processing and classification methodologies, the dynamic switching strategy, as well as the theological frame in which the system is embedded. Figure 2 shows the flow diagram of the proposed method.

2.1. Data collection and pre-processing

The dataset in this study contains 100 000 samples in total representing different weather conditions (fog, dust) and security threats (eavesdropping, jamming) for both FSO channel and RF channel. A list of features is used for each sample, for example, visibility range, SNR, and dust particle concentration. The authors' study uses a dataset with detailed measurements. For both technologies, baseline SNR and BER are included in the data [14, 15]. Moreover, the dataset is focused on the responses from the systems to adversarial manoeuvres like eavesdropping and jamming, thus providing a fresh angle on the subject of vulnerabilities. For every data point, environmental conditions in the form of levels of fog and dust, which are also known to affect optical transmissions, have been annotated [16]. This approach also enables a relative evaluation of the systems and their features under varying conditions, which, when coupled with SNR and BER measurements under different conditions, provides a holistic view on the operating efficacy of the systems and their capabilities vs. limitations in real scenarios. Given the data set as in the following equation [17]:

$$D = \{(xi, yi) \mid i = 1, 2, \ldots, N\}, \tag{1}$$

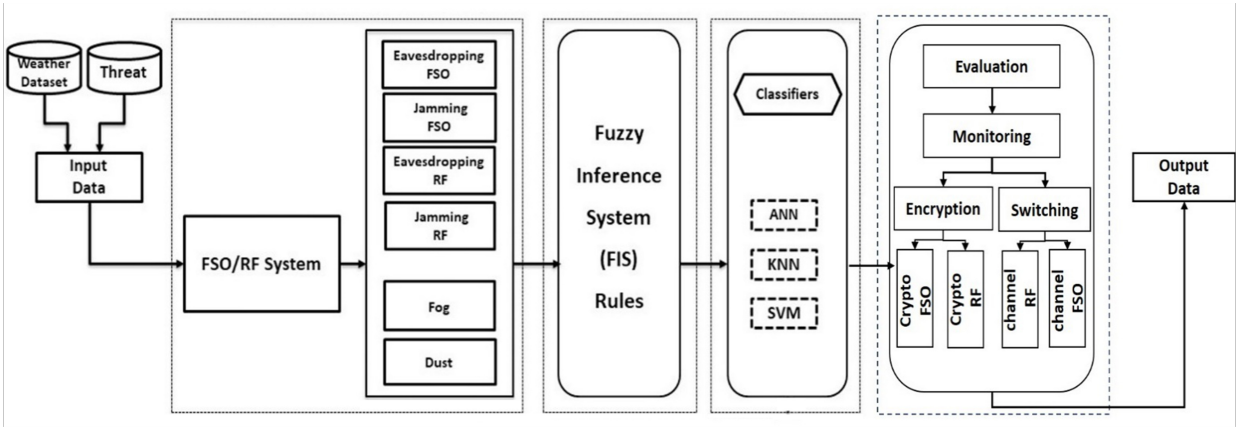


Fig. 2. Flow of the proposed method.

where *xi* represents the feature vector and *yi* represents the corresponding class label (weather condition or threat type), the data was split into training and testing sets using 60/40 ratio.

2.2. *Fuzzy logic for weather and threat classification*

In terms of data for the fuzzy rule-based classifier for FSO and RF communications systems, the data contains possible threats, as well as environmental effects including fog and dust [18]. Table 1 emphasizes that the fuzzy rules are evaluated for each situation: no threat ("NaN"), eavesdropping or jamming, environmental conditions from low to high and the attributes are assigned degrees of membership to these fuzzy sets [19]. The classification uses fuzzy logic to determine the degree to which real-world conditions fall into these categories accounting for the natural uncertainties present in environmental data. These membership values are combined via a fuzzy inference system (FIS) according to the fuzzy rules to evaluate the strength of each relevant rule. In the defuzzification stage, the evaluated rules are combined to arrive at a final recommendation for action; for example, under certain conditions like moderate fog and high dust, the system should opt for RF over FSO systems. It enables more flexibility in decision-making and effectively tackles the complexities introduced by different environmental factors that influence communication systems [20].

2.3. *Machine learning (ML) models for threat and weather classification*

The system leverages three ML models to classify weather conditions and security threats. These models are trained using pre-processed datasets to enhance the system predictive capabilities [21].

2.3.1. *k-nearest neighbours (KNN)*

FSO and RF communications systems implemented KNN algorithm for classifying the atmospheric conditions (fog and dust) and identifying the security threat (eavesdropping and jamming) [22]. KNN works based on seeing how the incoming data points relate to one of the training data points in the area. This approach calculates the Euclidean distance of each point in the dataset and finds the KNN [23]. KNN employs pattern detection to analyse variations in SNR and BER that could signify an unauthorized intrusion or manipulation of the signal in the context of eavesdropping detection. The algorithm classifies a signal as potentially compromised if the signal is close enough to examples of eavesdropping in the training set [24]. Jamming detection in KNN follows this example, recognizing an anomaly in the signals, which will generate the most similar patterns to the previously defined jamming specifications. KNN is used for weather classification; it is important for assessing the effect of fog and dust on signal quality in FSO systems. The fundamental operations of KNN are grounded in the computation of the Euclidean distance, defined mathematically as [25, 26]:

$$(x,y) = \sqrt{\sum_{i=1}^{n}\left(x_i - y_i\right)^2}, \tag{2}$$

where x and y are the data points with n dimensions. Following the distance calculation, the algorithm employs a majority voting system to classify a test point based on the most frequent category among its k [27]:

$$\text{Class}(x) = \text{Mode}\left\{\text{Class}\left(y_1\right), \text{Class}\left(y_2\right), \text{Class}\left(y_k\right)\right\}. \tag{3}$$

These equations underline KNN operational mechanism, facilitating its ability to provide reliable predictions and classifications. This adaptability makes KNN a highly efficient tool in managing the complex and dynamic challenges faced by FSO/RF communications systems, particularly under adverse weather conditions and security threats.

2.3.2. *Support vector machine (SVM)*

SVM is wildly used in the FSO and RF communication because it can classify the data very precisely and it can handle the non-linear relationship between classes. SVM separates the classes with a maximum margin hyper-plane that finds a position in the higher-dimensional space; therefore, it is efficient in classifying weather and security threats in a communication system [28]. In the security scenarios, the SVM is used to distinguish between normal and compromised signals based on the defined standard features such as SNR and BER, which can identify the threats of potential eavesdropping and jamming. For weather challenges, especially in FSO systems, it uses historical information to predict effects of specifics like fog

Table 1.
Fuzzy rules for action classification in FSO and RF systems.

No	FSO-Threat	RF-Threat	Fog	Dust	Action	No.	FSO-Threat	RF-Threat	Fog	Dust	Action
1	NaN	NaN	Moderate	High	**RF**	28	Eavesdropping	Jamming	High	High	**Crypto RF**
2	NaN	NaN	Moderate	Moderate	**FSO**	29	Eavesdropping	Jamming	High	Moderate	**Crypto RF**
3	NaN	NaN	Moderate	Severe	**RF**	30	Eavesdropping	Jamming	High	Severe	**Crypto RF**
4	NaN	NaN	High	High	**RF**	31	Eavesdropping	Eavesdropping	Moderate	High	**Crypto RF**
5	NaN	NaN	High	Moderate	**RF**	32	Eavesdropping	Eavesdropping	Moderate	Moderate	**Crypto FSO**
6	NaN	NaN	High	Severe	**RF**	33	Eavesdropping	Eavesdropping	Moderate	Severe	**Crypto RF**
7	NaN	Jamming	Moderate	High	**Crypto RF**	34	Eavesdropping	Eavesdropping	High	High	**Crypto RF**
8	NaN	Jamming	Moderate	Moderate	**FSO**	35	Eavesdropping	Eavesdropping	High	Moderate	**Crypto RF**
9	NaN	Jamming	Moderate	Severe	**Crypto RF**	36	Eavesdropping	Eavesdropping	High	Severe	**Crypto RF**
10	NaN	Jamming	High	High	**Crypto RF**	37	Jamming	NaN	Moderate	High	**RF**
11	NaN	Jamming	High	Moderate	**Crypto RF**	38	Jamming	NaN	Moderate	Moderate	**RF**
12	NaN	Jamming	High	Severe	**Crypto RF**	39	Jamming	NaN	Moderate	Severe	**RF**
13	NaN	Eavesdropping	Moderate	High	**Crypto RF**	40	Jamming	NaN	High	High	**RF**
14	NaN	Eavesdropping	Moderate	Moderate	**Crypto FSO**	41	Jamming	NaN	High	Moderate	**RF**
15	NaN	Eavesdropping	Moderate	Severe	**Crypto RF**	42	Jamming	NaN	High	Severe	**RF**
16	NaN	Eavesdropping	High	High	**Crypto RF**	43	Jamming	Jamming	Moderate	High	**Crypto RF**
17	NaN	Eavesdropping	High	Moderate	**Crypto RF**	44	Jamming	Jamming	Moderate	Moderate	**Crypto FSO**
18	NaN	Eavesdropping	High	Severe	**Crypto RF**	45	Jamming	Jamming	Moderate	Severe	**Crypto RF**
19	Eavesdropping	NaN	Moderate	High	**RF**	46	Jamming	Jamming	High	High	**Crypto RF**
20	Eavesdropping	NaN	Moderate	Moderate	**RF**	47	Jamming	Jamming	High	Moderate	**Crypto RF**
21	Eavesdropping	NaN	Moderate	Severe	**RF**	48	Jamming	Jamming	High	Severe	**Crypto RF**
22	Eavesdropping	NaN	High	High	**RF**	49	Jamming	Eavesdropping	Moderate	High	**Crypto RF**
23	Eavesdropping	NaN	High	Moderate	**RF**	50	Jamming	Eavesdropping	Moderate	Moderate	**Crypto FSO**
24	Eavesdropping	NaN	High	Severe	**RF**	51	Jamming	Eavesdropping	Moderate	Severe	**Crypto RF**
25	Eavesdropping	Jamming	Moderate	High	**Crypto RF**	52	Jamming	Eavesdropping	High	High	**Crypto RF**
26	Eavesdropping	Jamming	Moderate	Moderate	**Crypto FSO**	53	Jamming	Eavesdropping	High	Moderate	**Crypto RF**
27	Eavesdropping	Jamming	Moderate	Severe	**Crypto RF**	54	Jamming	Eavesdropping	High	Severe	**Crypto RF**

and dust on the signal transmission and guarantee communication [29]. Recall that SVM uses kernel functions to project input data into a higher-dimensional space where they are linearly separable. The algorithm maximizes the decision function [30]:

$$f(x) = \text{sgn}(w \cdot x + b), \tag{4}$$

where w is the weight vector, x represents the input features, and b is the bias. This formulation helps maximize the separation margin between classes, ensuring robust classification and high accuracy.

2.3.3. *Artificial neural network (ANN)*

In this aspect, ANNs are especially efficient for FSO/RF communication and have thus been implemented for numerous tasks in such as weather forecasting and security monitoring [8, 31].

ANNs are designed to function like the human brain, but instead of thinking, layers of nodes or neurons identify patterns and relationships [32]. For example, in FSO and RF systems, ANNs address problems related to, e.g., atmospheric effects on signal propagation and communications security threats via eavesdropping or jamming by relying on data from previous experience [33]. They take in signal parameters such as amplitude and frequency to identify discontinuities or alterations in those properties that could signal security concerns and model the effects of weather on signal quality (e.g., dust or fog). The basic structure of an ANN includes [34]:

- Input layer: collects the raw data.
- Hidden layers: these layers, where the bulk of processing occurs, transform inputs based on assigned weights and biases.
- Output layer: produces the final prediction or classification.

Mathematically, the operation within an ANN can be described as follows [35]:

$$y = \sigma\left(W_x + b\right), \tag{5}$$

where x is the input vector, W represents the weight matrix, b is the bias vector, and σ denotes the activation function that introduces non-linearity, making it possible for the network to learn complex patterns.

2.4. *Model evaluation metrics*

In a classification model, each sample is assigned a predicted label (positive or negative) to determine its class. This assignment results in four possible outcomes for each sample: False Negatives (FN), where actual positive samples are incorrectly labelled as negative; True Positives (TP), where actual positive samples are correctly labelled as positive; False Positives (FP), where actual negative samples are incorrectly labelled as positive; True Negatives (TN), where actual negative samples are correctly labelled as negative [36]. Table 2 [37] shows the classification model evaluation metrics.

3. Experimental results

The proposed approach is based on a PC platform, Intel C i7-12650H (2.30 GHz, 16 CPUs), and 16 GB DDR5 RAM, as well as NVIDIA GeForce RTX 4060 TI GPU, MATLAB (R2023b). Various intelligent models, like KNN, SVM, and ANN, etc., have been employed for classifying threats and weather conditions impacting FSO, as well as RF communication systems. In this section, the authors will analyse the experimental performance of these models based on various metrics, such as Accuracy, Recall, Precision, false positive rate (FPR), and other measures. Confusion matrices, a receiver operating characteristic (ROC) and an area under the ROC curve (AUC) curves and other statistical measures provide a quantitative performance analysis. An analysis of the three models used to classify threats (eavesdropping an jamming) and weather conditions (fog and dust) for optical and wireless communication systems shows that ANN, as illustrated in Table 3, had the highest accuracy of 99.989%, KNN had the second highest accuracy at 99.991%, and SVM had the lowest accuracy at 99.928%. The deep learning feature allows ANN to adapt better to complex data than KNN,

Table 2.
Classification model evaluation metrics.

Metric	Formula	#
Accuracy	$\frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})}$	(6)
Error	1 – Accuracy	(7)
Precision	$\frac{\text{TP}}{(\text{TP} + \text{FP})}$	(8)
Recall (True Positive Rate)	TP/P	(9)
Specificity	TN/N	(10)
False Positive Rate (FPR)	1 – Specificity	(11)
F1 Score	$2 * \frac{(\text{ Precision } * \text{ Recall })}{(\text{ Precision } + \text{ Recall })}$	(12)
Matthews Correlation Coefficient (MCC)	$\frac{((\text{TP} * \text{TN}) - (\text{FP} * \text{FN}))}{\sqrt{((\text{TP} + \text{FP}) * (\text{TP} + \text{FN}) * (\text{TN} + \text{FP}) * (\text{TN} + \text{FN}))}}$	(13)
Cohen's Kappa	$\kappa = (\text{p\_0} - \text{p\_}e)/(1 - \text{p\_}e)$	(14)

Table 3
Classification results using algorithms (KNN, SVM, ANN).

ML	Accuracy	Error	Recall	Specificity	Precision	FPR	F1_score	MCC_ score	Kappa
KNN	0.99991	0	0.999	0.999949	0.99996	5.13189E-05	0.99961	0.999574824	1
ANN	0.99989	0	0.999	0.999972	0.99647	2.83363E-05	0.99776	0.997739662	1
SVM	0.99928	0	0.999	0.999625	0.9962	0.000374739	0.99744	0.997115266	0.998

whose basis of classification sits on comparing proximity and is affected by the size of the data, but has a fast prediction. Non-linearly separable or highly overlapping data is a challenging task for SVM, which results in a decrease in its classification efficiency.

This confusion matrix from Fig. 3 shows the classification accuracy of ANN was superior (ANN – 49 985 correct positive classifications and just five FN) when compared to KNN (49 980 TP, 10 FN) and SVM (49 950 TP, 35 FN). In Crypto FSO and Crypto RF, ANN outperforms other classifiers; it is intended to encrypt the channel where switching between the FSO and RF channel and *vice versa* is hindered and reduces errors significantly; KNN is close to its optimality, and SVM records the highest error rates. While ANN proved to offer better performance in FSO and RF, its reduction of false positives makes this model an effective one to identify weather and environmental threats.

For FPR according to Fig. 4, ANN shows the minimum at 0.0000283 with KNN at 0.0000513, and SVM at 0.0003747. The AUC values in Fig. 4 indeed confirm that ANN outperforms the most with an AUC value of 0.99997, followed closely by KNN (0.99995), and SVM (0.9996). ROC indicates close-to-perfect performance of Crypto FSO, Crypto RF, FSO, RF (AUC = 1), and also the most stable classification with ANN. KNN shows high precision but, with a very poor recall, slightly improves again on SVM. ANN has the ROC closest to the upper-left corner, marking higher sensitivity and precision, followed by KNN, and slightly behind is SVM.

4. Conclusions

This research proposed a method for determining the necessary action (monitoring, switching, and encryption) in the event of a threat or changing weather and established a structure based on AI algorithms to classify the acquired data to maintain the stability of the FSO/RF system. The authors suggested using the fuzzy logic technique to classify threats (eavesdropping, jamming) and weather (fog, dust), which amounted to 54 rules important for action classification in FSO and RF systems. Note that to generate the results of the authors' approach, three algorithms (KNN, ANN, and SVM) were utilized to classify the extracted rules. Furthermore, KNN, ANN, and SVM classifiers attained an accuracy of approximately 99%, indicating a substantial improvement in the predictive accuracy of the proposed approach compared to traditional approaches. ANN outperforms all of its counterparts, considering

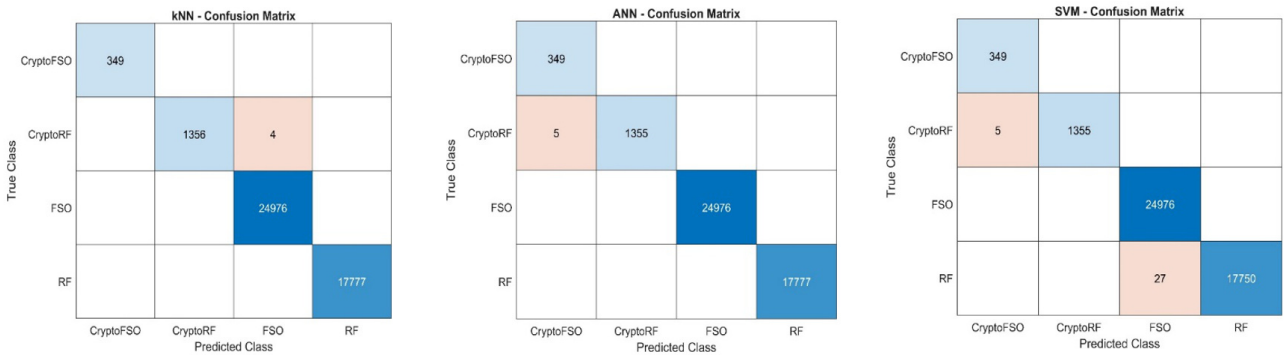


Fig. 3. Confusion matrices: KNN, ANN, SVM.

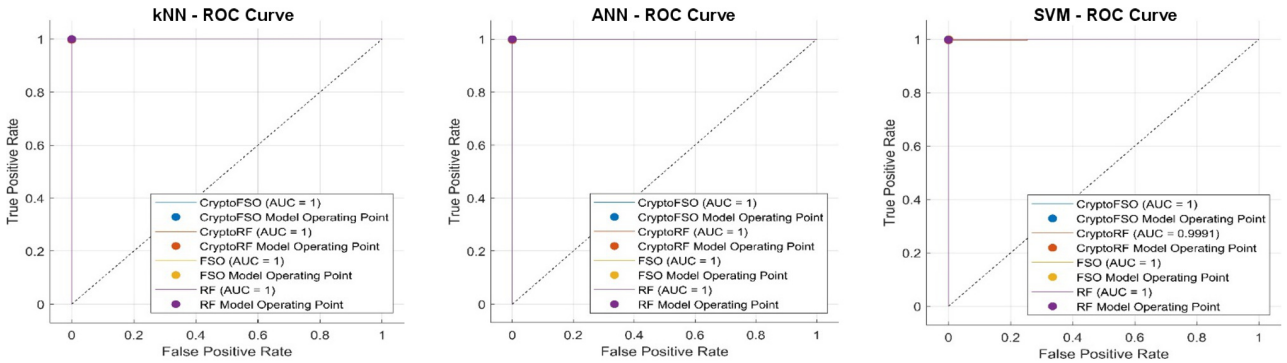


Fig. 4. ROC and AUC: KNN, ANN, SVM.

overall performance, obtaining high accuracy and a low error rate, with an optimal trade-off between precision and recall and the lowest false positive rate; it should be noted that complex AI algorithms, notably ANN, introduce computational delays, processing occurs at the system controller level, not along the data transmission path. This maintains the high-speed advantage of FSO (> 100 Gbps), as the AI cost (measured at less than 0.1 ms per decision) is negligible compared to the reduction in downtime caused by security or weather conditions (up to 35%). While KNN provides a similar performance, it is also more dependent on the size of the data, as well as needing careful tuning of the k parameter. In some cases, SVM is also effective, but it is relatively less efficient as it produces false positives more than from previous cases and exhibits a fall in discrimination capability. These outcomes indicate a definite conceptualization of the robustness and efficiency of the proposed method in recognizing threats or variations in climatic conditions, consequently allowing improved diagnosis in an earlier and more precise manner. This study prioritizes high-level decision efficiency over low-level physical signal analysis. Future work will integrate physics informed ML to capture effects like turbulence and polarization shifts under extreme environmental conditions.

References

[1] Alhosani, A., Alshehhi, F., Almenhali, M. & Abu Hilal, H. Optical communication advancements in free space and applications of free space orbital technology. *J. Inst. Eng. (India) B* **106**, 805–814 (2024). https://doi.org/10.1007/s40031-024-01137-5

[2] EL-Garhy, S. M., Khalaf, A. A., Aly, M. H. & Abaza, M. Intelligent transportation: a hybrid FSO/VLC-assisted relay system. *Opto-Electron. Rev.* **30**, e144260 (2022). https://doi.org/10.24425/opelre.2022.144260

[3] Aboelala, O., Lee, I. E. & Chung, G. C. A survey of hybrid free space optics (FSO) communication networks to achieve 5G connectivity for backhauling. *Entropy* **24**, 1573 (2022). https://doi.org/10.3390/e24111573

[4] Magidi, S. & Jabeena, A. Analysis of hybrid FSO/RF communication system under the effects of combined atmospheric fading and pointing errors. *Opt. Quantum Electron.* **54**, 210 (2022). https://doi.org/10.1007/s11082-022-03586-y

[5] Allaoua, O. *et al*. Optimizing FSO systems for 6G network using particle swarm optimization. *J. Opt. Commun*. **2024**, 0183 (2024). https://doi.org/10.1515/joc-2024-0183

[6] Khoshafa, M. H. *et al.* RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey. *IEEE Commun. Surv. Tutor* **99**, 1–1 (2024). https://doi.org/10.1109/COMST.2024.3487112

[7] Shakir, W. M. R. Physical layer security performance analysis of hybrid FSO/RF communication system. *IEEE Access* **9**, 18948–18961 (2020). https://doi.org/10.1109/ACCESS.2020.3048614

[8] Sefako, T., Yang, F., Song, J., Balmahoon, R. & Cheng, L. A Review of machine learning techniques for optical wireless communication in intelligent transport systems. *Intell. Converg. Networks* **5**, 284–316 (2024). https://doi.org/10.23919/ICN.2024.0019

[9] Ibrahim, M. *et al.* Anticipating Optical availability in hybrid RF/FSO links using RF beacons and deep learning. *IEEE Trans. Mach. Learn. Commun. Netw*. **2**, 1369–1388 (2024). https://doi.org/10.1109/TMLCN.2024.3457490

[10] Alimi, I. A. & Monteiro, P. P. Revolutionizing free-space optics: A survey of enabling technologies, challenges, trends, and prospects of beyond 5G free-space optical (FSO) communication systems. *Sensors* **24**, 8036 (2024). https://doi.org/10.3390/s24248036

[11] Shao, J., Liu, Y., Du, X. & Xie, T. Adaptive modulation scheme for soft-switching hybrid FSO/RF links based on machine learning. *Photonics* **11**, 404 (2024). https://doi.org/10.3390/photonics11050404

[12] Raj, A. A. B. *et al.* A review–unguided optical communications: Developments, technology evolution, and challenges. *Electronics* **12**, 1922 (2023). https://doi.org/10.3390/electronics12081922

[13] Jahid, A., Alsharif, M. H. & Hall, T. J. A contemporary survey on free space optical communication: Potentials, technical challenges, recent advances and research direction. *J. Netw. Comput. Appl.* **200**, 103311 (2022). https://doi.org/10.1016/j.jnca.2021.103311

[14] Deka, R., Mishra, V., Ahmed, I., Anees, S. & Alam, M. S. On the performance and optimization of HAPS assisted dual-hop hybrid RF/FSO system. *IEEE Access* **10**, 80976–80988 (2022). https://doi.org/10.1109/ACCESS.2022.3195930

[15] Kumar, S. & Sharma, N. Emerging military applications of free space optical communication technology: A detailed review. *J. Phys.: Conf. Ser.* **2161**, 012011 (2022). https://doi.org/10.1088/1742-6596/2161/1/012011

[16] Esmail, M. A., Ragheb, A. M., Fathallah, H. A., Altamimi, M. & Alshebeili, S. A. 5G-28 GHz signal transmission over hybrid all-optical FSO/RF link in dusty weather conditions. *IEEE Access* **7**, 24404–24410 (2019). https://doi.org/10.1109/ACCESS.2019.2900000

[17] Burkart, N. & Huber, M. F. A survey on the explainability of supervised machine learning. *J. Artif. Intell. Res.* **70**, 245–317 (2021). https://doi.org/10.1613/jair.1.12228

[18] Mohammadpour, R. A., Abedi, S. M., Bagheri, S. & Ghaemian, A. Fuzzy rule-based classification system for assessing coronary artery disease. *Comput. Math. Methods Med.* **2015**, 564867 (2015). https://doi.org/10.1155/2015/564867

[19] Minhas, A. A., Khan, M. S., Henna, S. & Iqbal, M. S. Attenuation-based hybrid RF/FSO link using soft switching. *Opt. Eng.* **60**, 56102 (2021). https://doi.org/10.1117/1.OE.60.5.056102

[20] Ahmadi, H., Gholamzadeh, M., Shahmoradi, L., Nilashi, M. & Rashvand, P. Diseases diagnosis using fuzzy logic methods: A systematic and meta-analysis review. *Comput. Methods Programs Biomed.* **161**, 145–172 (2018). https://doi.org/10.1016/j.cmpb.2018.04.013

[21] Hassan, M. M. *et al.* Machine learning-based rainfall prediction: Unveiling insights and forecasting for improved preparedness. *IEEE Access* **11**, 132196–132222 (2023). https://doi.org/10.1109/access.2023.3333876

[22] Tumma, Y. & Kappala, V. K. A review on deployment of UAV-FSO system for high-speed communication. *IEEE Access* **12**, 124915–124930(2024). https://doi.org/10.1109/ACCESS.2024.3453918

[23] Zhang. S. Challenges in KNN classification. *IEEE Trans. Knowl. Data Eng.* **34**, 4663–4675 (2021). https://doi.org/10.1109/TKDE.2021.3049250

[24] Jiang, W., Wang, J., Hsiung, K.-L. & Chen, H.-Y. GRNN-based detection of eavesdropping attacks in SWIPT-enabled smart grid wireless sensor networks. *IEEE Internet Things J.* **11**, 37381–37393 (2024). https://doi.org/10.1109/JIOT.2024.3443277

[25] Lonis, A. Experimental assessment of the atmospheric effects on laser communications on maritime environment. (Amitos University of the Peloponnese I.R, 2023). https://doi.org/10.26263/amitos-1693

[26] Halder, R. K., Uddin, M. N., Uddin, A., Aryal, S. & Khraisat, A. Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications. *J. Big Data* **11**, 113 (2024). https://doi.org/10.1186/s40537-024-00973-y

[27] Cunningham, P. & Delany, S. J. K-nearest neighbour classifiers-a tutorial. *ACM Comput. Surv*. **54**, 1–25 (2021). https://doi.org/10.1145/3459665

[28] Babatunde, K. S. *et al*. Machine Learning Model for Classifying Free Space Optics Channel Impairments. in *2022 5th Information Technology for Education and Development (ITED)* 1–8 (IEEE, 2002).

[29] Abdelsalam, N., Al-Kuwari, S. & Erbad, A. Physical layer security in satellite communication: State-of-the-art and open problems. *IET Commun.* **19**, e12830 (2025). https://doi.org/10.1049/cmu2.12830

[30] Chauhan, V. K., Dahiya, K. & Sharma, A. Problem formulations and solvers in linear SVM: A review. *Artif. Intell. Rev.* **52**, 803–855 (2019). https://doi.org/10.1007/s10462-018-9614-6

[31] Khudhair, K. T. *et al*. Soft Edge Detection by Mamdani Fuzzy Inference of Color Image. in *5th International Conference on Engineering Technology and its Applications (IICETA)* 379–383 (IEEE, 2022). https://doi.org/10.1109/IICETA54559.2022.9888456

[32] Kebaili, R., Driz, S. & Fassi, B. Tackling FSO-WDM system challenges with artificial neural networks: A comprehensive analysis. *Eurasia Proc. Sci. Technol. Eng. Math*. **32**, 304–310 (2024). https://doi.org/10.55549/epstem.1602779

[33] Puspitasari, A. A., An, T. T., Alsharif, M. H. & Lee, B. M. Emerging technologies for 6G communication networks: Machine learning approaches. *Sensors* **23**, 7709 (2023). https://doi.org/10.3390/s23187709

[34] Gupta, T. K. & Raza, K. Optimization of ANN architecture: A review on nature-inspired techniques. *ML Biosig. Anal. Diag. Imaging* **2019**, 159–182 (2019). https://doi.org/10.1016/B978-0-12-816086-2.00007-2

[35] Panić, M., Živković, Ž. & Veličković, M. Assessing the impact of the non-economic factors on gdp per capita using MLRA and ANNs. *Econ. Comput. Econ. Cybern. Stud. Res*. **56**, 187–201 (2022). https://doi.org/10.24818/18423264/56.3.22.12

[36] Najjar, F. H. *et al*. Classification of COVID-19 from X-ray images using GLCM features and machine learning. *Mal. J. Fund. Appl. Sci*. **19**, 389–398 (2023). https://doi.org/10.11113/mjfas.v19n3.2911

[37] Vujović, Ž. Classification model evaluation metrics. *Int. J. Adv. Comput. Sci. Appl*. **12**, 599–606 (2021). https://doi.org/10.14569/IJACSA.2021.0120670