ACS OMEGA

Open Access

http://pubs.acs.org/journal/acsodf

Article

VOC-Certifire: Certifiably Robust One-Shot Spectroscopic Classification via Randomized Smoothing

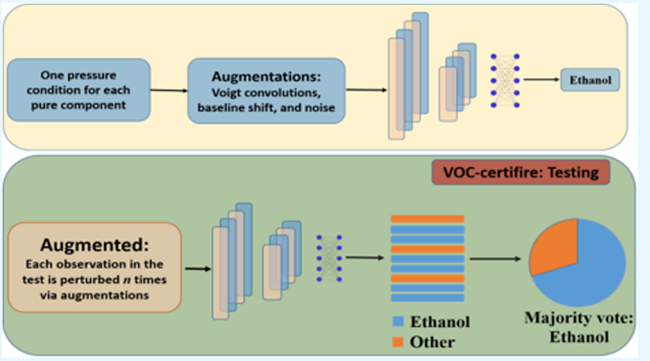
Mohamed Sy,* Emad Al Ibrahim, and Aamir Farooq*

Cite This: *ACS Omega* 2024, 9, 39033−39042

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: Spectroscopic methods are advantageous for gas detection with applications ranging from safety to operational efficiency. Despite the potential of laser-based sensors, real-world challenges, such as noise, interference and unseen conditions, hinder the accurate identification of species. The use of conventional machine learning (ML) models is constrained by extensive data requirements and their limited adaptability to new conditions. Although augmentation-based strategies have proven to improve the robustness of machine learning models, they still do not offer a complete defense. To address these challenges, this study focuses on three primary goals: first, to detect pressure-induced spectral broadening using simple yet effective augmentations; second, to bypass the need for extensive data sets by deploying a one-shot learning approach that can identify up to 12 volatile organic compounds (VOCs); and third, to provide a provable certification for the one-shot learning model predictions via randomized smoothing. To assess the effectiveness of our proposed augmentations and randomized smoothing, we perform a comparative study with four distinct models: VOC-net, VOC-lite, VOC-plus, and VOC-certifire. Remarkably, the one-shot learning model proposed herein, VOC-certifire, delivers predictions that match the baseline model VOC-net. The VOC-certifire predictions not only exhibit robustness and reliability but are also certified within a predefined l_2 norm radius. Such a certification is particularly useful for gas detection, where the robustness, precision and consistency are key to well-informed decision-making.



INTRODUCTION

Gas sensing is crucial in various sectors such as environment,[1,2] energy,[3,4] and healthcare,[5] significantly enhancing safety and operational efficiency.[6] Accurate and selective gas sensors are vital for the detection of hazardous substances, enabling effective decision-making and risk management. Researchers have explored various gas sensing techniques like photoacoustics,[7] electro-chemical methods,[8] and gas chromatography.[9] However, laser-based spectroscopy stands out because it can identify gases by their unique spectral "fingerprints".[10] This method is nonintrusive, cost-effective, and efficient for measuring the composition, pressure, velocity, and temperature of gas mixtures. However, identifying these spectral fingerprints can be tricky, especially when different gases have overlapping features in complex mixtures, and this issue gets more pronounced with the effect of pressure and/or Doppler broadening in real-world settings.

Recent advancements in gas sensing have incorporated machine learning (ML) models for both classification and regression.[6,11−20] These models aim to automate spectral identification by learning unique absorption features that serve as fingerprints for each molecule. However, existing ML models, typically trained on i.i.d. (independent and identically distributed) data sets with known conditions, can encounter substantial accuracy when subjected to small perturbations or when tested on unseen conditions.[21] The limitation of generalizing to unknown conditions poses a significant challenge. Data augmentation techniques emerge as compelling solutions to enhance the robustness of ML models against potential perturbations.[22] Widely employed in image classification,[23] augmentation strategies involve mirroring, flipping, rotating, and zooming the original images to augment the data set.[23,24]

In spectroscopy, augmentations typically involve introduction of noise[16,25−27] and/or baseline shifts[28] to the spectra. Other methods involve the application of extended multiplicative signal augmentation, addressing physical distortions arising from scattering and instrumental effects.[29] A notable example of the effectiveness of data augmentation in gas sensing is shown by

Received: June 20, 2024
Revised: August 20, 2024
Accepted: August 27, 2024
Published: September 4, 2024

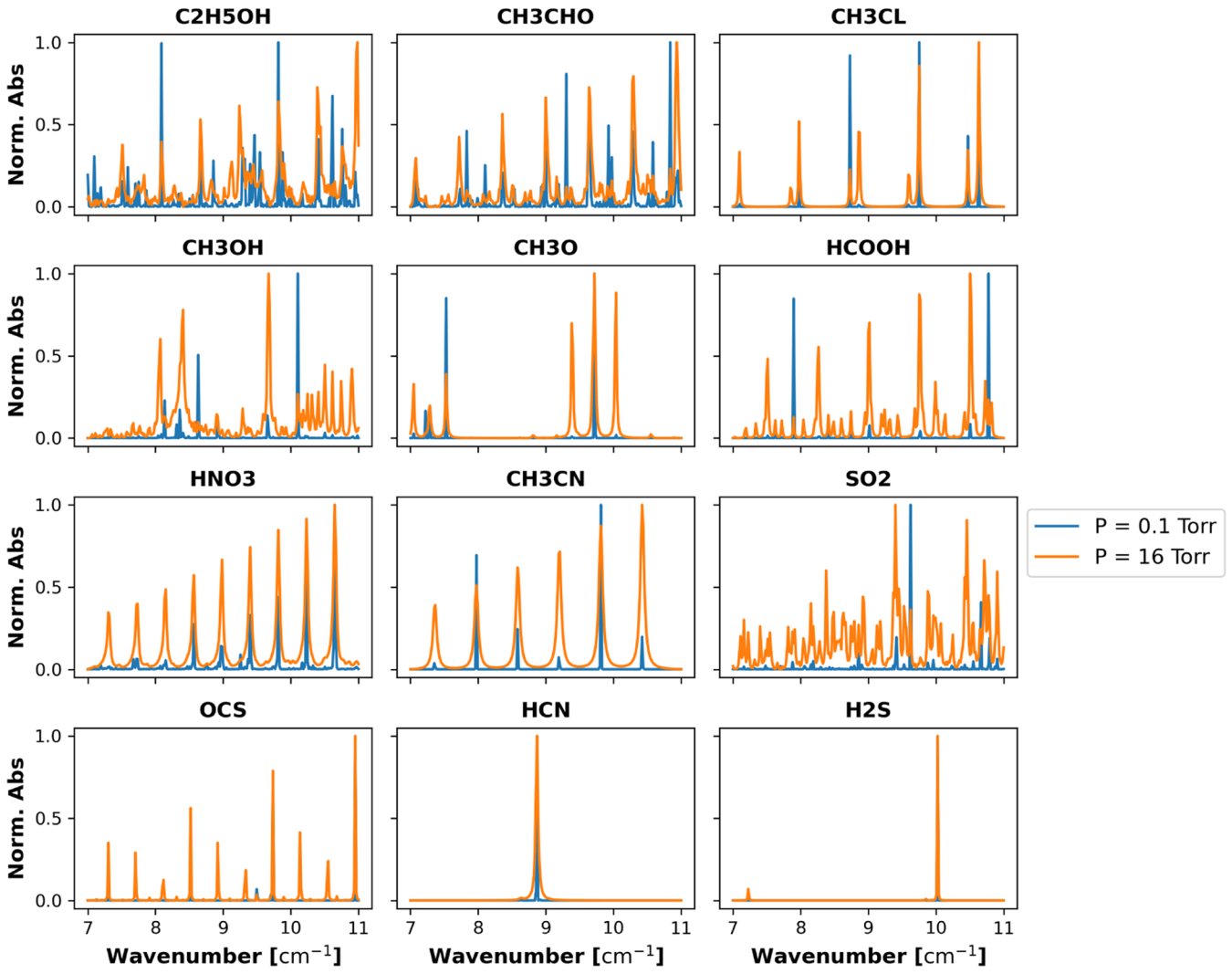


Figure 1. Normalized spectra of twelve VOCs at P = 0.5 Torr and P = 16 Torr.

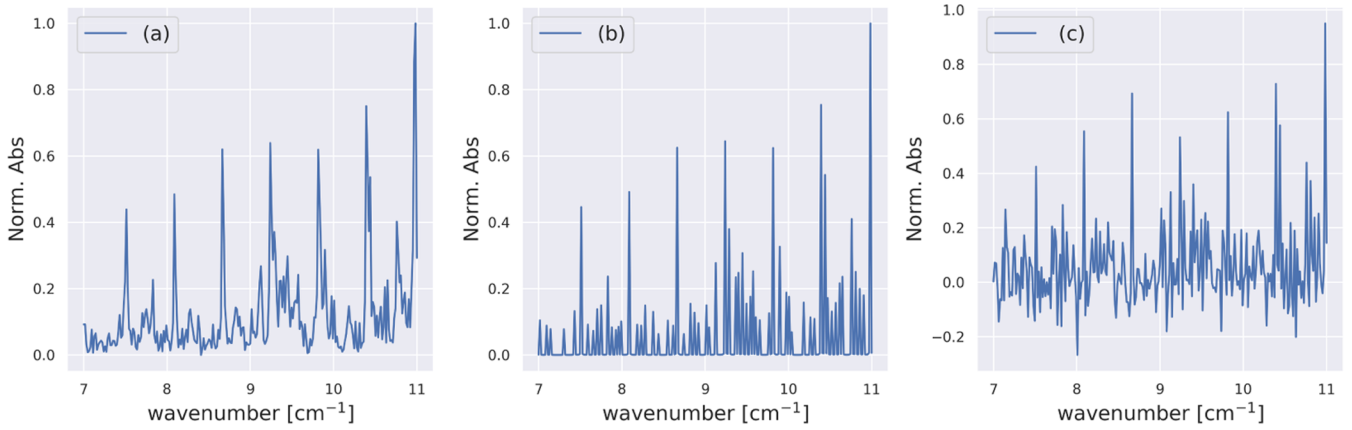
Al Ibrahim et al.[30] Their study introduces perturbations to composite spectra by adding fictitious spectra to the composite spectra through flipping, dilating, and mirroring the reference spectra, enhancing the model's generalization to unknown interferences. Despite their benefits, these augmentation techniques still require significant amounts of data to effectively train the ML models. This reliance on extensive data sets can be a limiting factor when such resources are not readily available.[31] In situations where a substantial amount of data is lacking, few-shot learning techniques can be employed.

In few-shot learning, the ML model is exposed to and trained on a limited data set (few examples), with the expectation that it can accurately predict unseen instances.[32] To put it simply, in the context of gas sensing, this entails training the machine learning model under a limited set of conditions of pressure and temperature (P, T), after which it is challenged to predict outcomes under different conditions (P, T). However, employing this approach poses challenges and may result in inaccurate predictions,[32,33] primarily due to the substantial variations in species spectra in response to the varying pressure and temperature conditions.[10,34] Factors such as Doppler-, self-, and collisional-broadening, along with line mixing, contribute significantly to these spectral variations.[10,34,35] Therefore, an augmentation technique that addresses these spectral variations is essential when adopting few-shot learning for precise predictions.[36] Existing spectroscopic augmentation methods fall short of capturing the dynamic changes in spectra caused by changes in pressure and temperature. To tackle these challenges, our study presents a new and straightforward augmentation method that effectively tackles spectral changes caused by variations in pressure and temperature.

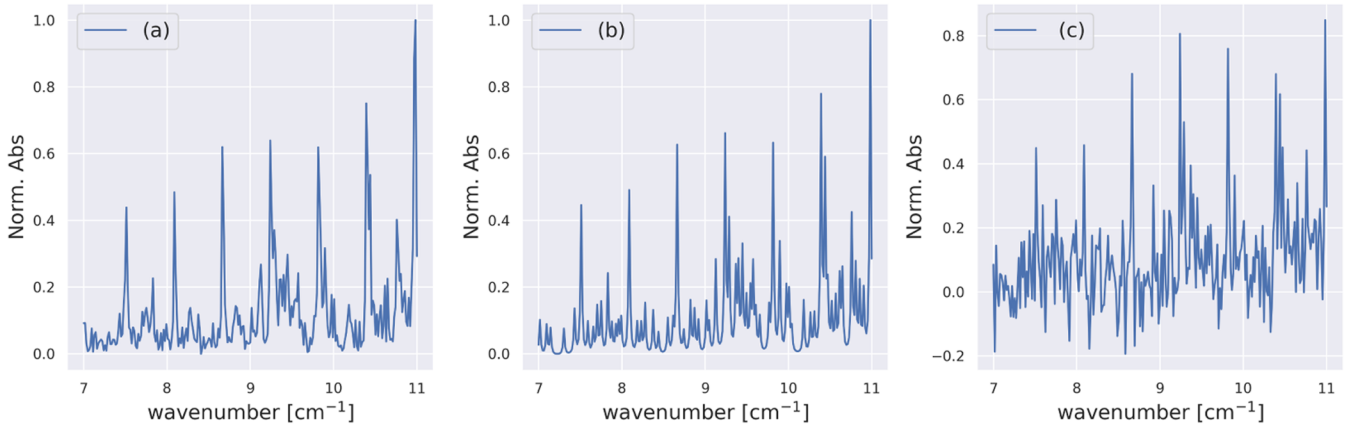
While augmentations contribute to improving the robustness of machine learning models, they do not provide complete defense against unseen perturbations/attacks.[37−39] In response to this limitation, various approaches have been developed to enhance a model's ability to defend itself against adversarial attacks. Many heuristic defenses have been proposed to create models resistant to adversarial perturbations; however, some of these defenses have proven vulnerable to more sophisticated adversaries.[37,40] Consequently, researchers have focused on strengthening empirical defenses[41] and developing certified defenses that offer robustness guarantees. Certified defenses ensure that classifiers deliver consistent predictions within a specified neighborhood of their inputs.[42−46]

In critical domains such as gas sensing, the importance of model robustness, repeatability, and accuracy cannot be overstated. Consequently, effective and trustworthy approaches become crucial for the precise detection of species, particularly

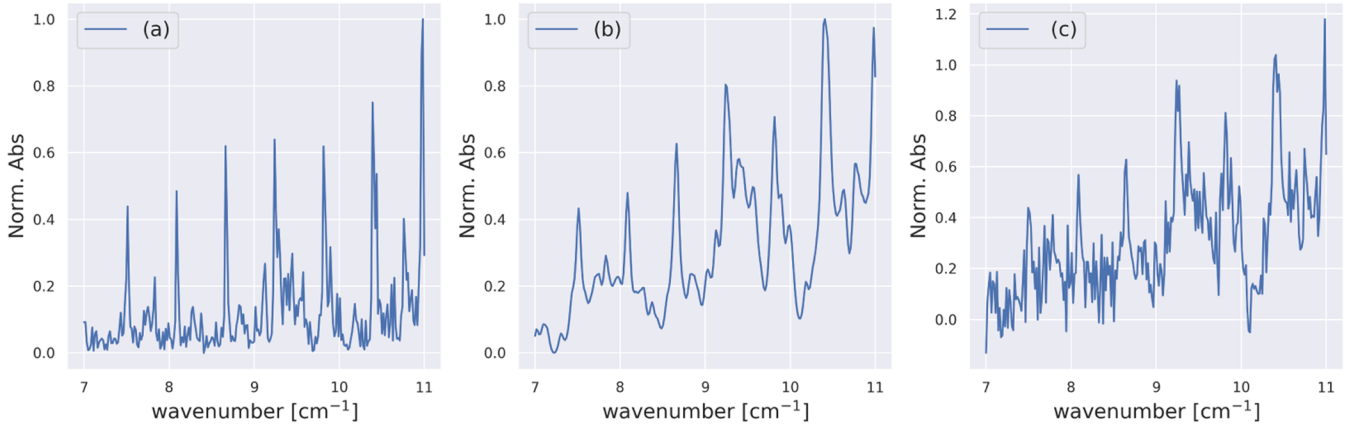
https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042



(1) Low FWHM Voigt augmentations for ethanol spectrum at P = 1 Torr



(2) Moderate FWHM Voigt augmentations for ethanol spectrum at P = 1 Torr



(3) High FWHM Voigt augmentations for ethanol spectrum at P = 1 Torr

Figure 2. Effect of augmentations across varied fwhm's. Common to all figures: (a) illustrates the normalized spectrum at $P = 1$ Torr, (b) showcases the augmented spectrum with Voigt convolutions, and (c) presents the same spectrum augmented with Voigt convolutions, noise, and baseline shifts.

toxic ones. Thus employing provably certifiable and robust classifiers such as those seen in[44,46] are necessary. The certification ensures that ML models can deliver reliable predictions within a predefined confidence radius, a crucial aspect in scenarios where precise and confident predictions are essential for decision-making and risk mitigation.

In this study, we focus on three key aspects: (1) introducing a novel augmentation technique which utilizes Voigt[47] convolutions with varying fwhm (full-width at half-maximum) to capture spectral changes due to pressure and temperature variations, in addition to noise and baseline shifts; (2) mitigating the need for extensive data by employing these augmentations to

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

create a one-shot learning model for species classifications; and (3) providing a provable certification for predictions made by the newly developed one-shot classification model through randomized smoothing.[44] We conduct a comprehensive comparison by classifying 12 volatile organic compounds (VOCs), replicating the VOC-net architecture from Chowdhury et al.;[20] our model is trained under a single condition and, through augmentations, demonstrates comparable accuracy. To further understand the impact of augmentations and randomized smoothing, we compare four models: VOC-net, VOC-lite, VOC-plus, and VOC-certifire. VOC-net, requiring a substantial amount of high-quality data, is trained with a stratified split under all pressure conditions, rendering it susceptible to unknown conditions. In contrast, VOC-lite, which shares the architecture with VOC-net, is trained solely on one pressure condition and is thus vulnerable to unknown conditions. VOC-plus undergoes training under a single pressure condition, leveraging Voigt augmentations for improved performance. Subsequently, VOC-certifire employs VOC-plus as its pretrained classifier. During the testing phase, randomized smoothing is implemented. This process entails subjecting each test spectrum to multiple perturbations through augmentations. The final prediction for VOC-certifire is determined by aggregating the majority vote from VOC-plus predictions applied to the perturbed spectra. A detailed analysis of the certification process is conducted, exploring how the relation between radius and certified accuracy varies based on the number of perturbations, noise level, and confidence level. VOC-certifire ensures robust and reliable predictions within predefined confidence bounds, thus providing a useful tool for decision-making in gas sensing applications.

METHODOLOGY

Data Set.

- **Simulated data**: To benchmark our one-shot learning models, a fair comparison with existing classification models is essential. Chowdhury et al.[20] introduced VOC-net, a convolutional neural network (CNN) model capable of classifying 12 VOCs, and evaluated its performance on both simulated and experimental data sets. In alignment with their approach, we chose to utilize a similar data set to facilitate a meaningful comparison and used their experimental data set for testing and validation. A concise overview of the VOC-net data set generation is provided here, with additional details on the experimental setup available in.[20]

  The training data for VOC-net was generated using spectral simulations of twelve VOCs. These simulations were carried out based on spectroscopic parameters extracted from the HITRAN[48] and JPL[49] databases, utilizing the HAPI tool[50] for spectral synthesis. Figure 1 illustrates representative normalized simulated spectra for each molecule at 0.5 and 16 Torr. The frequency range considered spans from 220 to 330 GHz (7.33−11 cm^{-1}). The data set encompasses spectra for the twelve VOC molecules, spanning a pressure range from 0.1 to 16.5 Torr (13.3−2200 Pa). Each spectrum corresponds to a single molecule and comprises 229 absorbance values, with a frequency resolution of 0.016 cm^{-1}.
- **Experimental Data:** Six VOCs were selected for experimental demonstration. Their spectra were obtained using an experimental setup, involving a THz microelectronics spectrometer operating in the 220−330 GHz range with a resolution of 0.5−15 MHz. Measurements were conducted in a gas cell with a 21.6 cm absorption path at room temperature. Absorbance was calculated with incident and transmitted intensities and applying the Beer−Lambert relation. The resulting experimental data set comprises 36 observations, with six measurements conducted for each of the six VOCs. Detailed information on the experimental setup can be found here.[20]
- **Augmentations**: In one-shot learning models, where training exclusively occurs under a singular pressure condition, the incorporation of augmentations becomes paramount. This necessity arises from the intrinsic data hunger of machine learning models and the need to address pressure-induced spectral variations, as depicted in Figure 1. Our augmentations extend beyond addressing noise and baseline shifts. Notably, they involve the convolution of Voigt profiles with varying full-width at half-maximum (fwhm). Voigt profiles, fundamental in spectroscopic modeling,[51] result from the convolution of Lorentzian and Gaussian profiles. Gaussian width reflects Doppler broadening due to temperature-induced particle motion, while Lorentzian width indicates broadening resulting from collisions or nonthermal effects.[34,35,51] The fwhm values, influenced by both Lorentzian (θ) and Gaussian (γ) widths, serve as indicators of pressure and temperature effects. Higher fwhm values signify elevated pressures and temperatures, leading to increased spectral line broadening. Conversely, lower values denote tighter lines, indicative of conditions at lower pressures and temperatures.[34,35] The dynamic interplay of both θ and γ, spanning from 0.001 to 0.05, facilitates the representation of spectral variations induced by changes in pressure and temperature. This comprehensive approach ensures that the augmentations effectively encapsulate the diverse spectral variations arising from varying conditions. Figure 2 illustrates augmentations for ethnol spectra at P = 1 Torr, in three cases, where θ and γ are small (0.001), moderate (0.01) and high (0.05). For higher pressures, the Voigt augmentation parameters can be adjusted to account for increased broadening, thereby capturing the spectral changes induced by elevated pressures, as detailed in the Supporting Information.

Machine Learning Models. In the upcoming sections, we will explore each model, offering insights into their architectures, training methodologies, and test data sets. For enhanced clarity and convenient reference, unique names have been assigned to each model. Table 1 succinctly summarizes the developed models along with their respective characteristics.

VOC-net and VOC-lite. An identical one-dimensional (1-D) CNN VOC classifier developed in[20] was replicated for both VOC-net and VOC-lite. Only a brief description of the model architecture is given below. Further details on hyperparameter tuning and model optimizations can be found here.[20] VOC-net

Table 1. VOC Models and Their Characteristics

models	training data	augmentations	certified
VOC-net	all pressures	no	no
VOC-lite	one pressure	no	no
VOC-plus	one pressure	yes	no
VOC-certifire	one pressure	yes	yes

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

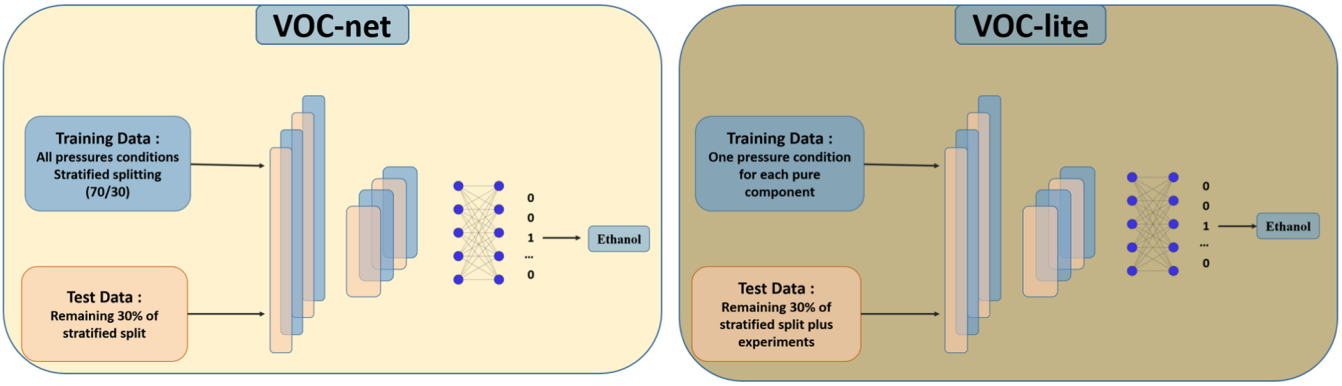


Figure 3. Schematic of VOC-net and VOC-lite training and testing procedures.

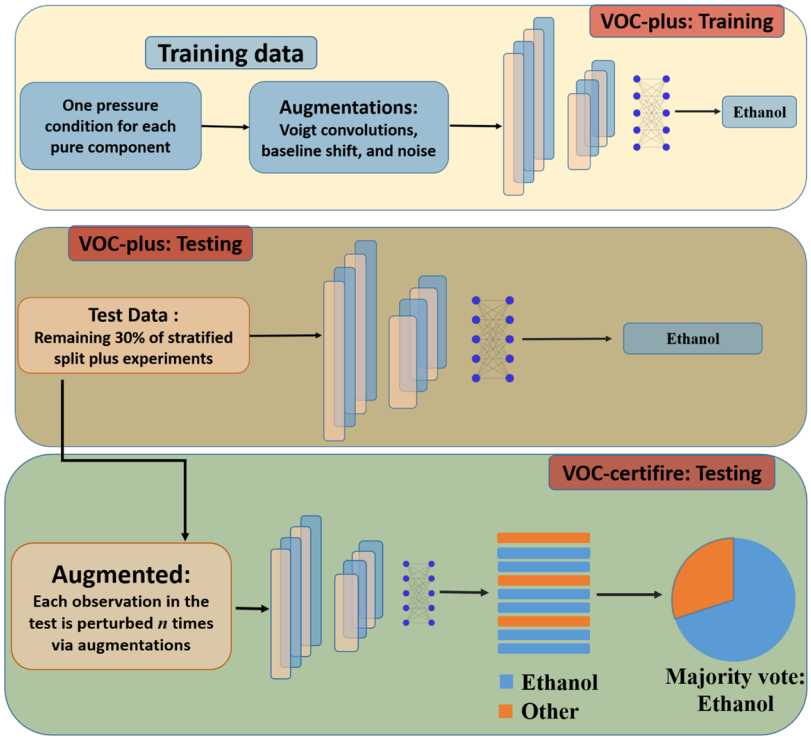


Figure 4. Schematics of training and testing procedure of VOC-plus and VOC-certifire.

relies on a 1-D CNN, comprising two convolutional layers, each with three filters of kernel size three. A subsampling (pooling) layer is strategically positioned between the convolutional layers. This is followed by a flattened dense layer, a hidden layer housing 48 neurons, and an output layer featuring 12 neurons, each corresponding to a distinct VOC species.

VOC-net serves as the baseline model, and it undergoes training across all pressure conditions (0.1−16.5 Torr) using a (70:30) stratified splitting approach to ensure a balanced distribution between training and test data. The training data set consists of 1377 simulated spectra of 12 VOCs at different pressure conditions, while the test data set comprises 591 simulated spectra of the same VOCs across various pressures. Additionally, 36 experimental spectra of six VOCs are included in the test data set; details of the experimental setup can be found in.[20] Conversely, VOC-lite shares the same architecture as VOC-net but is trained under a singular pressure condition, specifically at P = 1 Torr. Accordingly, the training data for VOC-lite consists of 12 observations, aiming for one-shot learning without augmentations. Schematic of the training and testing procedures for both VOC-net and VOC-lite is shown in Figure 3. To ensure a fair comparison, the test data are kept consistent across all models.

VOC-plus and VOC-certifire. The VOC-plus 1-D CNN architecture shares a similar structure with VOC-net, featuring a series of convolutional layers with ReLU activation and max-pooling to extract hierarchical features from one-dimensional molecular data. VOC-plus and VOC-net differ primarily in their training data sets. The training data set for VOC-plus comprises of each VOC at a single pressure, followed by augmentations. Augmentations involve various transformations on each VOC spectrum, including convolutions with Voigt profiles featuring varying Gaussian and Lorentzian widths (ranging from 0.0001 to 0.05), baseline shifts, and different noise levels. Each spectrum is augmented 1000 times, resulting in a total of 12,000 augmented components for model training. The test data are the same as used for VOC-net and VOC-lite. Details of the training costs for all the VOC models are provided in the Supporting Information.

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

As illustrated in Figure 4, VOC-certifire employs the pretrained VOC-plus model as its base classifier during training but takes a different path during testing. Notably, VOC-certifire incorporates randomized smoothing during its testing. This process involves perturbing each observation in the test data multiple times using the aforementioned augmentations before feeding it to the pretrained VOC-plus model. The final prediction of VOC-certifire is determined by the majority vote of the pretained classifier predictions for these perturbed instances. In simpler terms, if 100 perturbations are applied through augmentations to a test spectrum, and the model predicts 80 instances as ethanol and 20 instances as another substance, the majority vote rule designates the underlying test spectrum to be ethanol.

Randomized Smoothing. Let a classifier (f) map inputs from (R^d) to classes in (Y). The randomized smoothing procedure transforms the base classifier (f) into a smoothed classifier (g). Specifically, for a given input (x), (g) identifies the class most likely to be predicted by (f) under isotropic Gaussian noise perturbations of (x). Mathematically, this is expressed as

$$g(x) = \arg\max_{c \in Y} \mathbb{P}[f(x + \delta) = c], \text{ where } \delta \sim \mathcal{N}(0, \sigma^2 \mathrm{I}) \tag{1}$$

Here, the noise/perturbation level σ governs the tradeoff between robustness and accuracy. An increase in σ enhances the robustness of the smoothed classifier but reduces its standard accuracy.

A detailed robustness guarantee for the smoothed classifier g was initially introduced by.[44] They proposed an efficient algorithm rooted in Monte Carlo sampling to facilitate both prediction and certification. The robustness guarantee relies on the Neyman−Pearson lemma.[52] The procedure involves classifying $\mathcal{N}(x, \sigma^2 I)$ with the base classifier f, where class c_A is returned with probability $p_A = \mathbb{P}(f(x + \delta) = c_A)$, and the runner-up class c_B is returned with probability $p_B = \max_{c \neq c_A} \mathbb{P}(f(x + \delta) = c)$. The smoothed classifier g is deemed robust around x within a radius R, defined as

$$R = \sigma^2(\Phi^{-1}(p_A) - \Phi^{-1}(p_B)) \tag{2}$$

where Φ^{-1} is the inverse of the standard Gaussian cumulative distribution function. In Figure 5, a binary classifier certification is depicted. The red/blue half-spaces represent the decision regions in the smoothed classifier g obtained by majority voting of the base classifier f. The smoothed classifier g ensures consistent predictions within an l_2 circle with radius R, as indicated by the black circle, showing the certified robustness radius R of eq 2, as guaranteed by eq 1. On the right, it illustrates that for any $r > R$, there exists a perturbation δ with $\|\delta\|_2 = r$ such that $g(x + \delta) \neq g(x)$. This implies that robustness is only guaranteed within the circle of radius R.

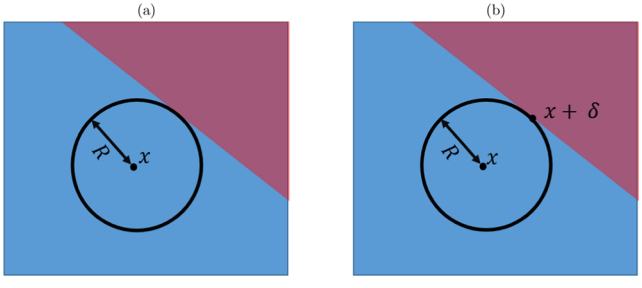


Figure 5. (a) The red and blue half-spaces represent the decision regions in the smoothed classifier g. The black circle is the robustness radius R. (b) For any $r > R$, there exists a perturbation δ with $\|\delta\|_2 = r$ such that $g(x + \delta) \neq g(x)$.

RESULTS AND DISCUSSION

To evaluate the performance of our models, we employed three key metrics: accuracy, F1-score, and precision. Detailed equations for these metrics are provided in the Supporting Information accompanying this paper. A concise overview of our findings is provided in Table 2 which presents a comparison of the aforementioned metrics for various models evaluated on both simulated and experimental data sets.

Table 2. Comparison of Different VOC Classification Models

	accuracy		F1-score		precision	
models	simul (%)	exp (%)	simul (%)	exp (%)	simul (%)	exp (%)
VOC-net	97.4	88.8	96.6	89.2	97.3	91.2
VOC-lite	47.5	50.2	35.6	40.5	31.7	38.8
VOC-plus	81.7	65	83	61	93.7	63
VOC-certifire	99	94	99	96	100	100

VOC-net and VOC-lite Results. Figures 6 and 7 showcase the outcomes of the baseline model, VOC-net, and its counterpart, VOC-lite. While both models share the architecture of VOC-net, VOC-lite is trained under a single pressure condition (P = 1 Torr). The accuracy experiences a significant drop for both experimental and simulated data for VOC-lite. This decline highlights the limited ability of the VOC-lite model to generalize to unseen pressure conditions.

The critical factor contributing to VOC-net's successful generalization and high accuracy is its comprehensive training across all pressure conditions (0−16.5 Torr). In the experimental data, VOC-net exhibits only three misclassifications among 36 observations, whereas VOC-lite exhibits 30 misclassifications. This stark contrast emphasizes VOC-lite's inability to generalize across different pressure and temperature conditions, indicating a failure to capture the spectral variations induced by changes in operating conditions.

VOC-plus and VOC-certifire Results. Figures 8 and 9 depict confusion matrices for VOC-plus and VOC-certifire models, evaluated on simulated and experimental data. VOC-plus is trained under a single pressure condition (P = 1 Torr) with augmentations (Voigt convolutions, noise, and baseline shifts). Noticeable improvements are observed, with VOC-plus achieving a significant increase in accuracy compared to VOC-lite, rising from 47.5 to 81.7% in simulated data. Additionally, VOC-plus exhibits 18 misclassifications compared to VOC-lite's 30 in experimental data. This underscores the efficacy of augmentations. VOC-certifire showcases remarkable accuracy, surpassing VOC-plus and achieving accuracy level comparable to the baseline model, VOC-net. In experimental data, VOC-certifire incurs one misclassification out of 36 observations. Despite utilizing VOC-plus as its pretrained classifier, VOC-certifire distinguishes itself by incorporating randomized smoothing during testing. This involves subjecting each observation in the test data set to multiple perturbations via augmentations, including Voigt convolutions, noise, and baseline shifts. The final prediction for VOC-certifire is determined by the majority vote of the pretrained classifier predictions on the perturbed instances. A notable strength of

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

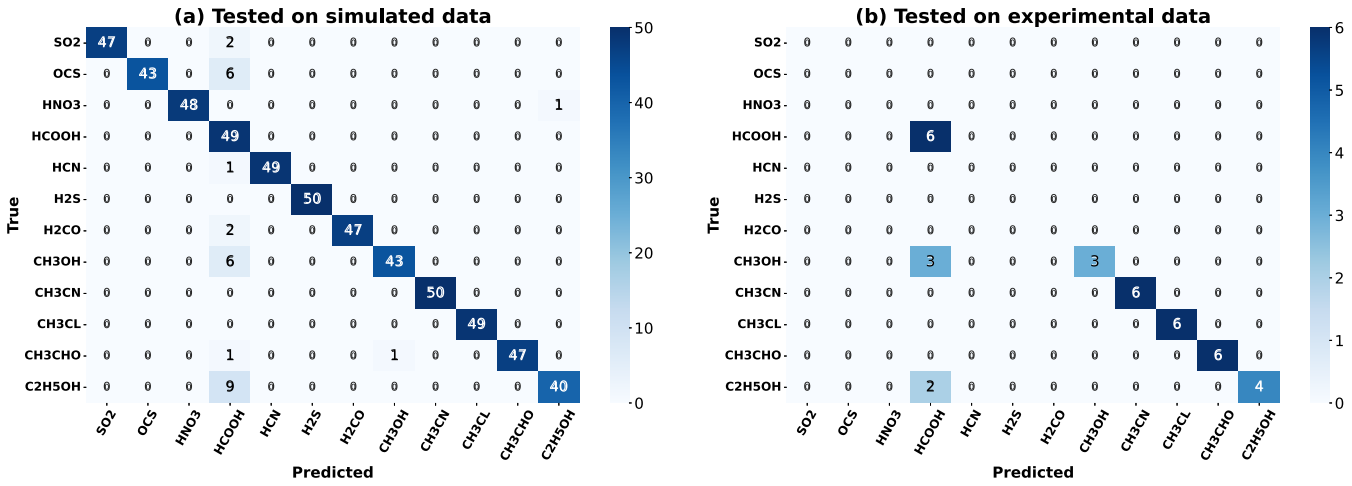


Figure 6. VOC-net confusion matrix. (a) Simulated data; (b) Experimental data.

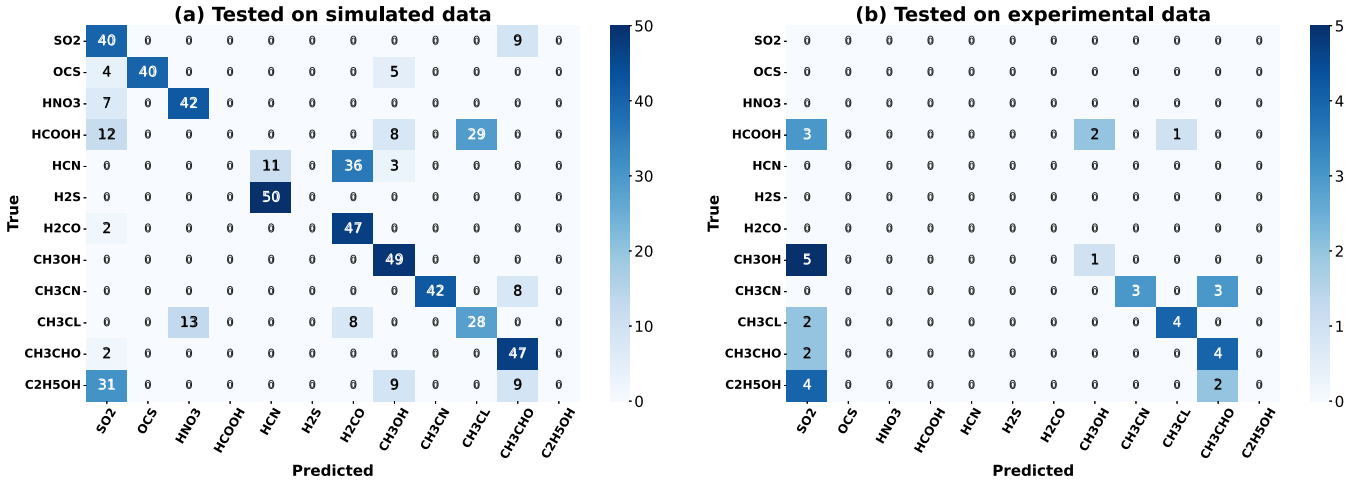


Figure 7. VOC-lite confusion matrix. (a) Simulated data; (b) Experimental data.

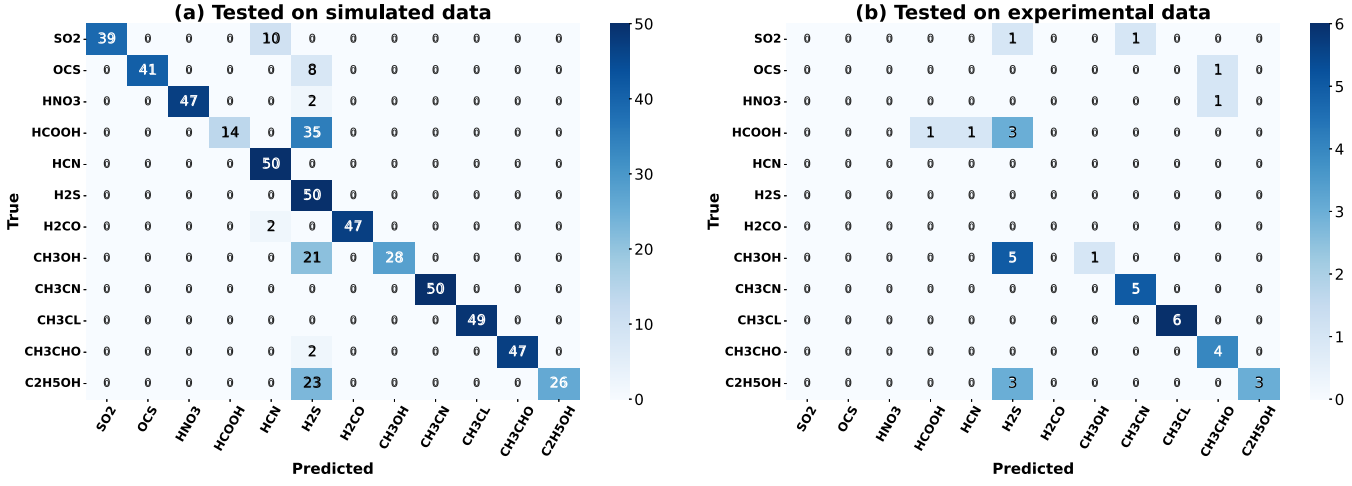


Figure 8. VOC-plus confusion matrix. (a) Simulated data; (b) Experimental data.

VOC-certifire lies in its certifiability, assuring robustness under perturbations and ensuring consistent predictions even in the face of uncertainties.

Model Certification. The smoothed classifier g is guaranteed to produce consistent predictions within an l_2 circle of radius R, centered at observation (x), as illustrated by eq 2. We assessed certified accuracy across different l_2 radii by varying parameters (α, σ and N). Figure 10a demonstrates the certified accuracy achieved through smoothing with varying σ for a fixed α (99.9%) and fixed N (1000), showcasing how σ plays a role in a robustness/accuracy tradeoff. Lower perturbation level σ values enable the certification of small radii with high accuracy,

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

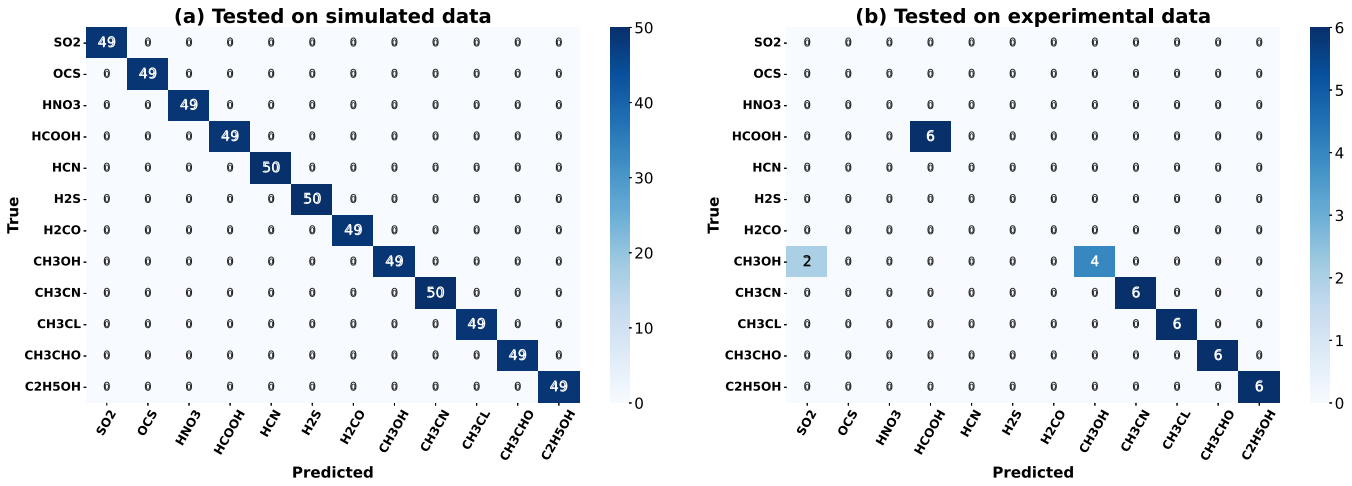
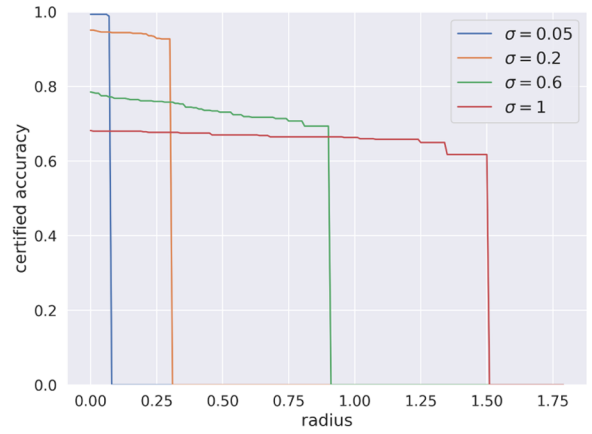
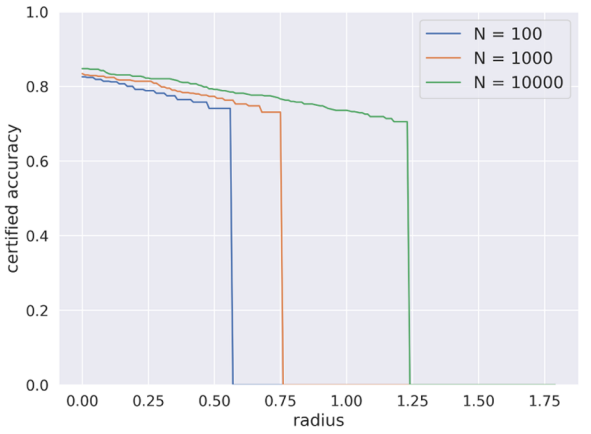


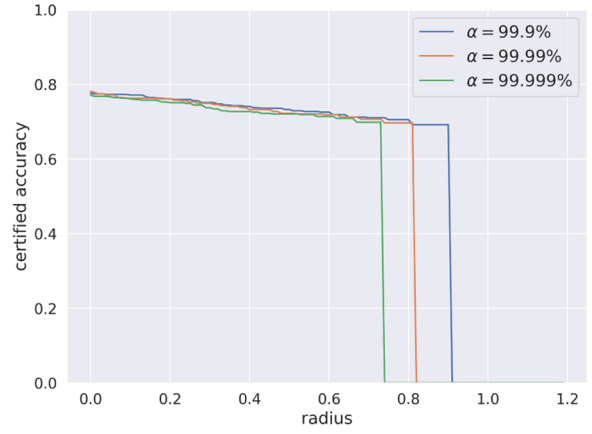
Figure 9. VOC-certifire confusion matrix. (a) Simulated data; (b) Experimental data.



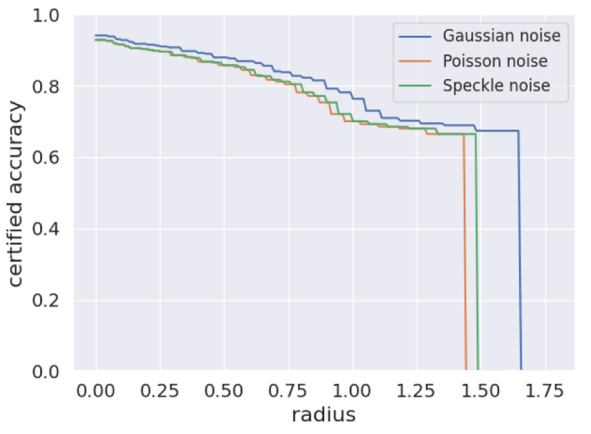
(a) Impact of σ (0.05 to 1) on certified accuracy vs radius



(b) Impact of N (100 to 10000) on certified accuracy vs radius



(c) Impact of α (99.9% to 99.99%) on certified accuracy vs radius



(d) Impact of different noise types on certified accuracy vs radius

Figure 10. Certified accuracy analysis.

while larger radii exhibit lower certification accuracy. Conversely, higher σ values facilitate the certification of larger radii but result in reduced accuracy for smaller radii, aligning with the findings in[44] regarding the tradeoff between adversarial attacks and standard accuracy. Figure 10b provides insights into how certified accuracy would change with varying randomized sample sizes N while σ and α are fixed. Higher samples size results in higher certification radius. Figure 10c illustrates the

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042

impact of varying the confidence level parameter α on certified accuracy while the sample size N and σ are fixed, highlighting its relatively low sensitivity to changes in α. Finally, Figure 10d assesses certified radius across different noise types, showing that the model, despite being trained only on Gaussian noise, maintains similar accuracy for unseen noise types.

CONCLUSIONS AND KEY HIGHLIGHTS

In this study, we explored VOC classification models, starting with VOC-net and VOC-lite, highlighting the significance of comprehensive training data for accurate generalization. To overcome the challenge of extensive data requirements, we introduced one-shot learning models coupled with straightforward yet impactful augmentations. These augmentations were designed to effectively capture pressure-induced spectral variations for both low and high pressures, faithfully representing real-world applications. We introduced VOC-plus, a one-shot learning model utilizing these augmentations during training, which yielded a significant improvement in accuracy compared to VOC-lite. Furthermore, we introduced VOC-certifire, a certifiable model that leverages VOC-plus as its base classifier through randomized smoothing. VOC-certifire demonstrated high accuracy in comparison to the baseline model, highlighting its robust and certified nature, ensuring consistent predictions even under unforeseen adversarial attacks.

The randomized smoothing procedure played a crucial role in certifying the robustness of VOC-certifire model. We conducted a thorough evaluation of parameters such as perturbation level σ, sample size (N), and confidence level (α), offering insights into the tradeoff between robustness and accuracy. Summarized in Table 2, our results underscore the significance of augmentations in enhancing one shot-learning model performance, and model's robustness against unforeseen perturbations. This study not only offers a comparative analysis of VOC classification models but also provides valuable insights into the balance between the robustness and accuracy of machine learning models. These findings contribute to the advancement of developing trustworthy machine learning models, particularly crucial in gas sensing applications where reliability and accuracy are crucial for well informed decision-making and effective risk mitigation strategies. Future work will involve exploring mixture classifications using one-shot learning and investigating the impact of augmentations on handling unknown interference and pressure-induced spectral changes within mixtures.

ASSOCIATED CONTENT

Data Availability Statement

The VOC-certifire model is hosted at: https://github.com/SyMohamed/voc_certifire.

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsomega.4c05757.

Detailed explanations of the performance metrics, computational costs, and the model's adaptation to environmental conditions (PDF)

AUTHOR INFORMATION

Corresponding Authors

Mohamed Sy − *Physical Science and Engineering Division (PSE), King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia;* orcid.org/0000-0002-9411-5321; Email: mohamed.sy@kaust.edu.sa

Aamir Farooq − *Physical Science and Engineering Division (PSE), King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia;* orcid.org/0000-0001-5296-2197; Email: aamir.farooq@kaust.edu.sa

Author

Emad Al Ibrahim − *Physical Science and Engineering Division (PSE), King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia;* orcid.org/0000-0001-8595-5102

Complete contact information is available at: https://pubs.acs.org/10.1021/acsomega.4c05757

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

This work was funded by the Office of Sponsored Research at King Abdullah University of Science and Technology (KAUST), Saudi Arabia. E.A. acknowledges the support of the Ibn Rushd Postdoctoral Fellowship Program, administered by the King Abdullah University of Science and Technology (KAUST).

REFERENCES

(1) Dhall, S.; Mehta, B. R.; Tyagi, A. K.; Sood, K. A review on environmental gas sensors: Materials and technologies. *Sens. Int.* **2021**, *2*, No. 100116.

(2) Mhanna, M.; Sy, M.; Farooq, A. A selective laser-based sensor for fugitive methane emissions. *Sci. Rep.* **2023**, *13*, No. 1573.

(3) Elkhazraji, A.; Shakfa, M. K.; Abualsaud, N.; Mhanna, M.; Sy, M.; Marangoni, M.; Farooq, A. Laser-based sensing in the long-wavelength mid-infrared: chemical kinetics and environmental monitoring applications. *Appl. Opt.* **2023**, *62*, A46−A58.

(4) Sy, M.; Zou, J.; Adil, M.; Elkhazraji, A.; Mhanna, M.; Farooq, A. Laser-based speciation of isoprene thermal decomposition behind reflected shock waves. *Proc. Combust. Inst.* **2024**, *40*, No. 105460.

(5) Owen, K.; Farooq, A. A calibration-free ammonia breath sensor using a quantum cascade laser with WMS 2f/1f. *Appl. Phys. B* **2014**, *116*, 371−383.

(6) Feng, S.; Farha, F.; Li, Q.; Wan, Y.; Xu, Y.; Zhang, T.; Ning, H. Review on smart gas sensing technology. *Sensors* **2019**, *19*, No. 3760.

(7) Tomberg, T.; Vainio, M.; Hieta, T.; Halonen, L. Sub-parts-per-trillion level sensitivity in trace gas detection by cantilever-enhanced photo-acoustic spectroscopy. *Sci. Rep.* **2018**, *8*, No. 1848.

(8) Bakker, E.; Telting-Diaz, M. Electrochemical sensors. *Anal. Chem.* **2002**, *74*, 2781−2800.

(9) Eckenrode, B. A. Environmental and forensic applications of field-portable GC-MS: an overview. *J. Am. Soc. Mass Spectrom.* **2001**, *12*, 683−693.

(10) Farooq, A.; Alquaity, A. B.; Raza, M.; Nasir, E. F.; Yao, S.; Ren, W. Laser sensors for energy systems and process industries: Perspectives and directions. *Prog. Energy Combust. Sci.* **2022**, *91*, No. 100997.

(11) Nicolle, A.; Deng, S.; Ihme, M.; Kuzhagaliyeva, N.; Ibrahim, E. A.; Farooq, A. Mixtures Recomposition by Neural Nets: A Multi-disciplinary Overview. *J. Chem. Inf. Model.* **2024**, *64*, 597−620, DOI: 10.1021/acs.jcim.3c01633.

(12) Mhanna, M.; Sy, M.; Arfaj, A.; Llamas, J.; Farooq, A. Laser-based selective BTEX sensing using deep neural networks. *Opt. Lett.* **2022**, *47*, 3247−3250.

(13) Javed, U.; Ramaiyan, K. P.; Kreller, C. R.; Brosha, E. L.; Mukundan, R.; Sengupta, A. M.; Morozov, A. V. Quantification of gas concentrations in NO/NO2/C3H8/NH3 mixtures using machine learning. *Sens. Actuators, B* **2022**, *359*, No. 131589.

(14) Mhanna, M.; Sy, M.; Elkhazraji, A.; Farooq, A. Deep neural networks for simultaneous BTEX sensing at high temperatures. *Opt. Express* **2022**, *30*, 38550−38563.
(15) Schwarm, K. K.; Spearrin, R. M. Real-time FPGA-based laser absorption spectroscopy using on-chip machine learning for 10 kHz intra-cycle emissions sensing towards adaptive reciprocating engines. *Appl. Energy Combust. Sci.* **2023**, *16*, No. 100231.
(16) Sy, M.; Mhanna, M.; Farooq, A. Multi-speciation in shock tube experiments using a single laser and deep neural networks. *Combust. Flame* **2023**, *255*, No. 112929.
(17) Peng, P.; Zhao, X.; Pan, X.; Ye, W. Gas classification using deep convolutional neural networks. *Sensors* **2018**, *18*, No. 157.
(18) Mozaffari, M. H.; Tay, L.-L. In *Convolutional Neural Networks for Raman Spectral Analysis of Chemical Mixtures*, 2021 5th SLAAI International Conference on Artificial Intelligence (SLAAI-ICAI); IEEE, 2021; pp 1−6.
(19) Wang, C.-Y.; Ko, T.-S.; Hsu, C.-C. Interpreting convolutional neural network for real-time volatile organic compounds detection and classification using optical emission spectroscopy of plasma. *Anal. Chim. Acta* **2021**, *1179*, No. 338822.
(20) Chowdhury, M. A. Z.; Rice, T. E.; Oehlschlaeger, M. A. VOC-Net: ADeep Learning Model for the Automated Classification of Rotational THz Spectra of Volatile Organic Compounds. *Appl. Sci.* **2022**, *12*, No. 8447.
(21) Roelofs, R.; Shankar, V.; Recht, B.; Fridovich-Keil, S.; Hardt, M.; Miller, J.; Schmidt, L. A meta-analysis of overfitting in machine learning *Adv. Neural Inf. Process. Syst.*, **2019** *32*.
(22) Perez, L.; Wang, J. The Effectiveness of Data Augmentation in Image Cassification Using Deep Learning. 2017, arXiv:1712.04621v1. arXiv.org e-Print archive. https://doi.org/10.48550/arXiv.1712.04621.
(23) Shorten, C.; Khoshgoftaar, T. M. A survey on image data augmentation for deep learning. *J. Big Data* **2019**, *6*, No. 60.
(24) Cubuk, E. D.; Zoph, B.; Mane, D.; Vasudevan, V.; Le, Q. V. In *Autoaugment: Learning Augmentation Strategies from Data*, 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); IEEE, 2019; pp 113−123.
(25) Gan, L.; Yuen, B.; Lu, T. Multi-label classification with optimal thresholding for multi-composition spectroscopic analysis. *Mach. Learn. Knowl. Extr.* **2019**, *1*, 1084−1099.
(26) Barton, S.; Alakkari, S.; O'Dwyer, K.; Ward, T.; Hennelly, B. Convolution network with custom loss function for the denoising of low SNR Raman spectra. *Sensors* **2021**, *21*, No. 4623.
(27) Zhang, C.; Zhou, L.; Zhao, Y.; Zhu, S.; Liu, F.; He, Y. Noise reduction in the spectral domain of hyperspectral images using denoising autoencoder methods. *Chemom. Intell. Lab. Syst.* **2020**, *203*, No. 104063.
(28) Wahl, J.; Sjödahl, M.; Ramser, K. Single-step preprocessing of raman spectra using convolutional neural networks. *Appl. Spectrosc.* **2020**, *74*, 427−438.
(29) Blazhko, U.; Shapaval, V.; Kovalev, V.; Kohler, A. Comparison of augmentation and pre-processing for deep learning and chemometric classification of infrared spectra. *Chemom. Intell. Lab. Syst.* **2021**, *215*, No. 104367.
(30) Al Ibrahim, E.; Farooq, A. Augmentations for selective multi-species quantification from infrared spectroscopic data. *Chemom. Intell. Lab. Syst.* **2023**, *240*, No. 104913.
(31) Brigato, L.; Iocchi, L. In *A Close Look at Deep Learning with Small Data*, 2020 25th International Conference on Pattern Recognition (ICPR); IEEE, 2021; pp 2490−2497.
(32) Wang, Y.; Yao, Q.; Kwok, J. T.; Ni, L. M. Generalizing from a few examples: A survey on few-shot learning. *ACM Comput. Surv.* **2021**, *53*, 1−34.
(33) Seo, J.-W.; Jung, H.-G.; Lee, S.-W. Self-augmentation: Generalizing deep networks to unseen classes for few-shot learning. *Neural Networks* **2021**, *138*, 140−149.
(34) Goldenstein, C. S.; Spearrin, R. M.; Jeffries, J. B.; Hanson, R. K. Infrared laser-absorption sensing for combustion gases. *Prog. Energy Combust. Sci.* **2017**, *60*, 132−176.
(35) Hanson, R. K.; Spearrin, R. M.; Goldenstein, C. S. *Spectroscopy and Optical Diagnostics for Gases*; Springer, 2016; Vol. *1*.
(36) Altae-Tran, H.; Ramsundar, B.; Pappu, A. S.; Pande, V. Low data drug discovery with one-shot learning. *ACS Cent. Sci.* **2017**, *3*, 283−293.
(37) Carlini, N.; Wagner, D. In *Towards Evaluating the Robustness of Neural Networks*, 2017 IEEE Symposium on Security and Privacy (SP); IEEE, 2017; pp 39−57.
(38) Goodfellow, I. J.; Shlens, J.; Szegedy, C. Explaining and Harnessing Adversarial Examples. 2014, arXiv:1412.6572v3. arXiv.org e-Print archive. https://doi.org/10.48550/arXiv.1412.6572.
(39) Szegedy, C.; Zaremba, W.; Sutskever, I.; Bruna, J.; Erhan, D.; Goodfellow, I.; Fergus, R. Intriguing Properties of Neural Networks. 2013, arXiv:1312.6199v4. arXiv.org e-Print archive. https://doi.org/10.48550/arXiv.1312.6199.
(40) Athalye, A.; Carlini, N.; Wagner, D. In *Obfuscated Gradients give a False Sense of Security: Circumventing Defenses to Adversarial Examples*, Proceedings of the 35th International Conference on Machine Learning; PMLR, 2018; pp 274−283.
(41) Madry, A.; Makelov, A.; Schmidt, L.; Tsipras, D.; Vladu, A. Towards Deep Learning Models Resistant to Adversarial Attacks. 2017, arXiv:1706.06083v4. arXiv.org e-Print archive. https://doi.org/10.48550/arXiv.1706.06083.
(42) Raghunathan, A.; Steinhardt, J.; Liang, P. Certified Defenses against Adversarial Examples. 2018, arXiv:1801.09344v2. arXiv.org e-Print archive. https://doi.org/10.48550/arXiv.1801.09344.
(43) Wong, E.; Kolter, Z. In *Provable Defenses against Adversarial Examples via the Convex Outer Adversarial Polytope*, Proceedings of the 35th International Conference on Machine Learning; PMLR, 2018; pp 5286−5295.
(44) Cohen, J.; Rosenfeld, E.; Kolter, Z. In *Certified Adversarial Robustness via Randomized Smoothing*, Proceedings of the 36th International Conference on Machine Learning; PMLR, 2019; pp 1310−1320.
(45) Salman, H.; Li, J.; Razenshteyn, I.; Zhang, P.; Zhang, H.; Bubeck, S.; Yang, G. Provably robust deep learning via adversarially trained smoothed classifiers *Adv. Neural Inf. Process. Syst.* 2019; Vol. *32*.
(46) Salman, H.; Sun, M.; Yang, G.; Kapoor, A.; Kolter, J. Z. Denoised smoothing: A provable defense for pretrained classifiers. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 21945−21957.
(47) Olivero, J. J.; Longbothum, R. L. Empirical fits to the Voigt line width: A brief review. *J. Quant. Spectrosc. Radiat. Transfer* **1977**, *17*, 233−236.
(48) Gordon, I. E.; Rothman, L. S.; Hill, C.; Kochanov, R. V.; Tan, Y.; Bernath, P. F.; Birk, M.; Boudon, V.; Campargue, A.; Chance, K. V.; et al. The HITRAN2016 molecular spectroscopic database. *J. Quant. Spectrosc. Radiat. Transfer* **2017**, *203*, 3−69.
(49) Pickett, H. M.; Poynter, R. L.; Cohen, E. A.; Delitsky, M. L.; Pearson, J. C.; Müller, H. S. P. Submillimeter, millimeter, and microwave spectral line catalog. *J. Quant. Spectrosc. Radiat. Transfer* **1998**, *60*, 883−890.
(50) Kochanov, R. V.; Gordon, I. E.; Rothman, L. S.; Wcisło, P.; Hill, C.; Wilzewski, J. S. HITRAN Application Programming Interface (HAPI): A comprehensive approach to working with spectroscopic data. *J. Quant. Spectrosc. Radiat. Transfer* **2016**, *177*, 15−30.
(51) Whiting, E. E. An empirical approximation to the Voigt profile. *J. Quant. Spectrosc. Radiat. Transfer* **1968**, *8*, 1379−1384.
(52) Neyman, J.; Pearson, E. S. IX. On the Problem of the most Efficient Tests of Statistical Hypotheses. In *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*; The Royal Society London, 1933; Vol. *231*, pp 289−337.

https://doi.org/10.1021/acsomega.4c05757
ACS Omega 2024, 9, 39033−39042