Information and Networking Event
Horizon Europe 2023-2024 Calls
Co-Funded by the Government of India (DST)

HORIZON-CL4-2024-HUMAN-03-02: Explainable and Robust AI

24 May 2024

Quantiles are Versatile: Robust and Interpretable Machine Learned System using Quantile based Uncertainty Quantification

- Name of presenter: Snehanshu Saha **(w/ Santonu Sarkar, Aditya Challa, Sravan Danda, Sougato Sen, Surjyo Ghosh)**
- Birla Institute of Technology and Science Pilani, K K Birla Goa Campus, India (Private University, Institute of Eminence)
- Contact details: Email- snehanshus@goa.bits-pilani.ac.in; Ph: +91-6366331331
- Web url: https://universe.bits-pilani.ac.in/goa/snehanshus/profile

Quantile based Robust Inferencing

Existing Sigmoid & Binary cross entropy CAN'T capture the uncertainty of the latent function $f(x)$

Quantiles can!

- $\rho(f_{\tau(x)} > f(x) = \tau$
- $P(y = 1|f_\tau(x)) \equiv \begin{cases} 1 - \tau e^{(\tau-1)f(x)}, 0 < f_\tau(x) \\ (1-\tau)e^{\tau f(x)}, 0 \geq f_\tau(x) \end{cases}$
- **This can be defined as the negative log-likelihood function, which allows to capture quantiles of the latent.**

IEEE TAI 2022

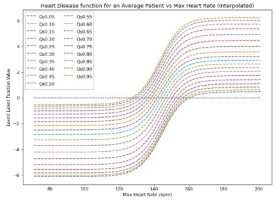
Helps in uncertainty quantification

Improves Robustness

Lipschitz constant for quantile regression using neural networks

$\frac{K_z * max(\tau, 1-\tau)}{m}$; $K_z = max_j \, ||a_j^{[L-1]}||$ $\tau = quantile$ (Gene Expression Inference)

- Can capture whether or not there are samples of opposite classes ($f_\tau(x) > 0$ or ≤ 0)
- Can find how far away from the median the class label changes
- Confidence score (δ) is correlated with miss classification rate ($\delta, 0.5 - \delta$); further augmented with Lipschitz acceleration



IEEE/ACM TCBB 2023

Quantile Probability

UAI 2024

- Assuming that the data is generated using $y = I[f(x) + \epsilon]$ where $f(x)$ is a pre-trained classifier we predict $P(y = 1) = \int_{\tau=0}^{1} I[\mathbb{Q}(x, \tau) \geq 0.5]d\tau$
- As a result, we can
  - make Deep Neural Networks reliable.
  - decouple loss function from Quantile representation.
  - obtain quantile probabilities from any $f(x)$
  - preserve calibration errors across distortions

Achieves generalization

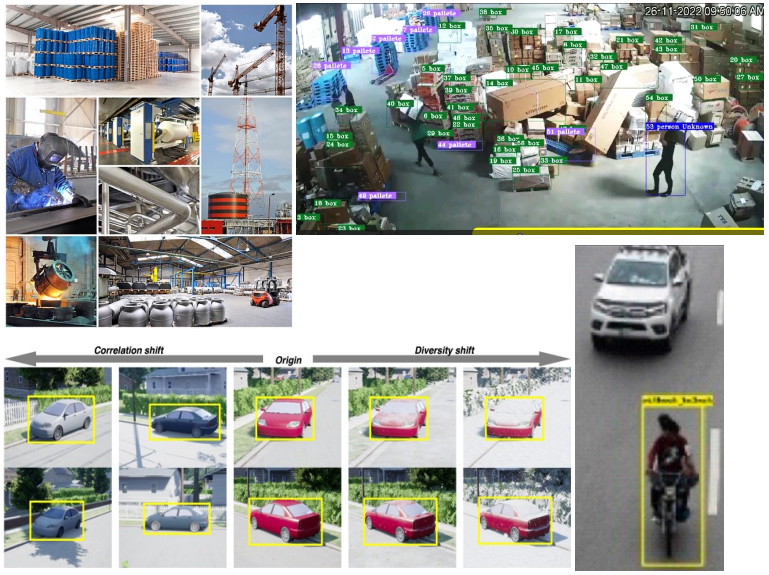
Makes a Classifier Distortion invariant

Quantile Activation can be agnostic to distortion, as a result,

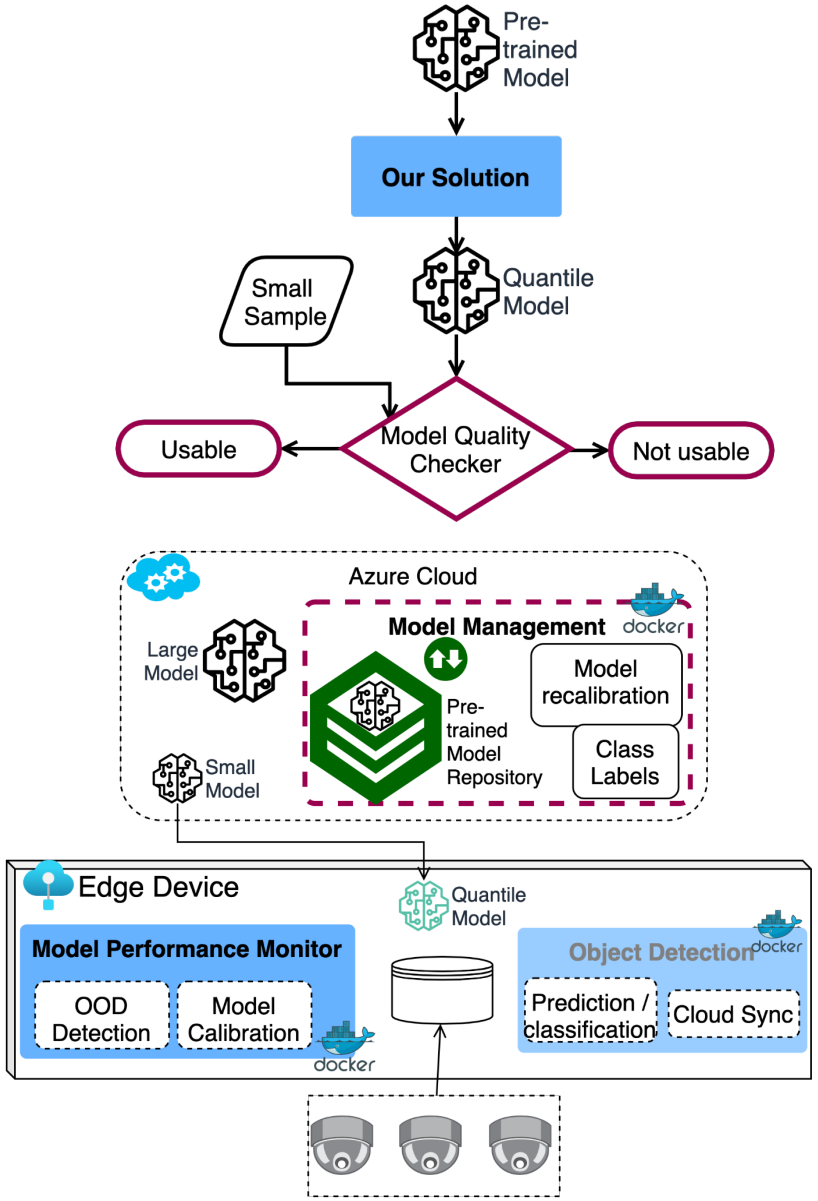
- needs minimal retraining for a shifted dataset
- Out -of- distribution detection

Arxiv 2024

Application Scenario 1-Object detection



Our (quantile-wrapped) model corrects base classifier(pre-trained models) for object detection (Safety hazards, T & L, Traffic Safety)



Application Scenario 2-Anomaly Detection

Anomaly Detection in Time-series data using Quantile LSTM

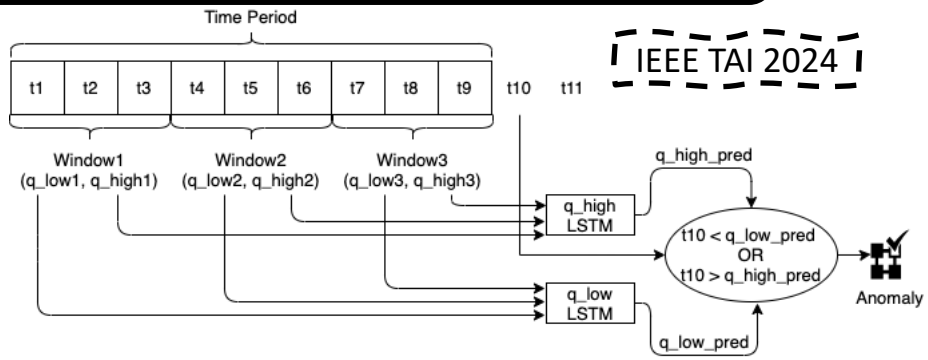
- A time-series dataset D comprises a set of time periods T_k, each partitioned into a set of windows w
- For a T_k, $X_{k,\tau} \equiv \{\mathbb{Q}_\tau(T_k^j), j = 1, \cdots, w\}$ as predictors and $Y_{k,\tau} \equiv \mathbb{Q}_\tau(T_{k+1})$, as the response at a future timestep

1. Estimate quantile $Q_\tau(x_{k+t+1})$ with $\tau \in (0,1)$
2. Define a statistic to measure the outlier-ness of the data, given the observation x_{k+t+1}

- Compute two quantiles q_{low} and q_{high} from the current windows to forecast them in the next time period
- Anomalies are those lying outside this range

Benefits

- Distribution invariant
- Thresholds are adaptive, they change depending on quantiles
- Can detect even a singleton anomaly; beats many SOTA algorithms



IEEE TAI 2024

Going Forward (with Quantiles)

- Multivariate Anomaly Detection (Geometric Quantiles)—addresses current limitation
- ZERO calibration error across distortions!
- **On-device, lightweight anomaly and object** detection

•HORIZON-CL4-2024-HUMAN-03-02: Explainable and Robust AI (24 May 2024)
Co-Funded by the Government of India (DST)

Quantiles are Versatile: Robust and Interpretable Machine Learned System using Quantile based Uncertainty Quantification

- Consortium: Snehanshu Saha **w/ Santonu Sarkar, Aditya Challa, Sravan Danda, Sougato Sen, Surjyo Ghosh;** Anuradha and Prashanth Palakurthi Centre for Artificial Intelligence Research (APPCAIR) and Dept. of CSIS, Birla Institute of Technology and Science Pilani, K K Birla Goa Campus, India (Private University, *Institute of Eminence*)
- Type of cooperation sought: Scientific and Scholarly (Academic within EU)
- Collaboration Profile: Statisticians and Computer Scientists with interest and demonstrated evidence of expertise in Uncertainty Quantification and On Device learning in Deep Neural Networks
- Experience: Demonstrated evidence of solving problems in UQ and on Device Learning (Since 2018)
- Keywords: *Quantile Activation, Departure from single point estimation, Context distribution, Adversarial Effects of Data Corruption, Duality, Object and OOD detection, Anomaly detection*