ECE Graduate Research Seminars-Summer 2024

In Person Sessions: June 3-4, 2024

Remote Sessions: June 17-18, 2024

June 3, 2024-Morning Session

Name: Leah Krehling
Area of Research: Software Engineering
Supervisor: Dr. Aleksander Essex

Privacy Preserving Rule Matching

Private Set Intersection (PSI) is a secure multiparty computation cryptographic technique that enables two parties to compute the intersection of their data sets without revealing any information about the sets to each other. Existing PSI protocols typically assume that both parties have sets of equal size. However, in many real-world scenarios, the sets may be unbalanced, with one party having a much larger set than the other. Additionally, protocols focused on the unbalanced setting make assumptions about the larger set, which limits their applications. We propose an RSA-based protocol for unbalanced private set intersection that is efficient and secure in the data streaming setting. Our protocol minimizes the computational and communication costs incurred by set owners while providing strong privacy guarantees. The protocol is based on RSA, a widely-used public-key cryptosystem, and leverages homomorphic encryption and secure hashing to protect the privacy of the sets.

Name: Tristan Curry
Area of Research: Biomedical Systems
Supervisor: Abbas Samani

Using Tissue Mechanics Priors for Prostate Ultrasound Elastography

In Canada prostate cancer is one of the most common forms of cancer among males, with over 50,000 cases reported each year. Common forms of prostate cancer detection include a Prostate Specific Antigen (PSA) test, where a blood test is performed to determine if the amount of PSA is elevated. This can be problematic however, as a heightened level of PSA is not necessarily correlated with the presence of prostate cancer. Additionally, a Digital Rectal Exam (DRE) can be performed by clinicians, to determine if enlarged or stiffened regions of the prostate are present. The DRE test has a low sensitivity and can often produce erroneous results. Finally, Magnetic Resonance Elastography (MRE) methods, while reasonably accurate, are often time consuming and costly, precluding the possibility of broad clinical utility. To overcome these potential issues, we propose the use of Ultrasound technology to accurately track tissue displacements allowing for the mapping of tissue stiffness across the prostate. To acquire the required displacement data, a quasi-static mechanical stimulation is used through a transrectal ultrasound probe where a clinician acquires a pre- and post-compression radiofrequency dataset. This pair of radiofrequency datasets will be used in a 2-Dimensional analytical minimization algorithm formulated in the polar system to compute an initial estimate of the displacements. This initial estimate is refined using a strain refinement algorithm founded on tissue mechanics principle before a highly accurate tissue displacement field is estimated. Both algorithms required alterations to work with the polar datasets produced by the transrectal ultrasound transducers. In-silico radiofrequency data has been used with the algorithms to determine the accuracy of the algorithms outputs by comparing to known ground truth finite element models, providing an improvement of the strains from the initial guess and refinement algorithms. From these strains, a stiffness reconstruction algorithm can be used to generate improved elastography images that clinicians can use to help identify prostate tumors.

Name: Mohammad Noorchenarboo
Area of Research: Software Engineering
Supervisor: Katarina Grolinger

Explainable Anomaly Detection for Time Series Energy Data

Anomaly detection in energy systems is crucial for efficient energy management, enabling the identification of unusual consumption patterns that may indicate inefficiencies, faults, or external influences. This research introduces an innovative framework for explainable anomaly detection in time series energy data, focusing on enhancing the interpretability and actionable insights of identified anomalies. By leveraging a combination of statistical analysis, machine learning, and deep learning techniques, the framework aims to provide comprehensive explanations for various types of anomalies, facilitating improved decision-making processes in energy systems management. This approach not only addresses the detection of anomalies but also emphasizes the importance of context in understanding the underlying causes of these irregularities, offering a significant advancement in the field of energy data analytics.

Name: Amanda de Oliveira Timotheo
Supervisor: Miriam Capretz
Area of Research: Software Engineering

The Power of GANs for Image Dataset Augmentation

In the realm of computer vision and machine learning, augmenting image datasets holds considerable importance in improving both model performance and generalization capabilities. Among diverse methodologies, Generative Adversarial Networks (GANs) have emerged as a potent tool for achieving these enhancements. This methodology is composed of two neural networks, the Generator Network and the Discriminator Network, engaged in a min-max game to collaboratively improve performance. During the joint training, the Generator Network learns how to create samples similar to the desired image dataset, while the Discriminator Network enhances its ability to classify between a real sample and a generated sample. This workflow idea results in a powerful and elegant methodology to generate new samples to increase image datasets. Since the GAN concept was present in 2014, subsequent research has further refined and expanded upon the initial framework. This presentation will provide a concise overview of the use of GANs for augmenting image datasets, presenting some papers to illustrate a piece of the state-of-the-art in this domain. The primary objective of this presentation is to provide insight into the efficacy of GANs, highlighting some successful GAN-based methods employed over the years. The results from these selected papers underscore the remarkable capabilities of GANs in augmenting image datasets, demonstrating unparalleled effectiveness in enriching training datasets and improving model robustness.
Keywords: GANs, Image Generation, Data Augmentation.

Name: Mounika Pratapa
Supervisor: Aleksander Essex
Area of Research: Software Engineering

Leveraging Homomorphic Encryption for Privacy Preserving Genomic Data Analysis

The reduced cost of genome sequencing has opened up significant potential for genetic research. However, ethical and privacy concerns prohibit the free sharing of genomic data across institutions. Cryptography offers powerful tools like homomorphic encryption, which enables the performance of computations on encrypted data. Although fully homomorphic encryption (FHE) is a relatively new area within cryptography, developing practical implementations of FHE based schemes is crucial for creating privacy-preserving medical applications, such as secure genomic data sharing and machine learning. FHE schemes rely on lattice-based cryptography, making them secure against post-quantum cryptographic attacks. Nevertheless, they also face the challenge of noise growth during encrypted additions or multiplications, limiting the number of computations that can be performed while still allowing correct decryption. Machine learning applications require a large number of computations, thus requiring suitable optimizations for their implementation within the FHE framework. In this talk, I will discuss about FHE for machine learning, by introducing an application we developed called P-AutoImpute. This novel, privacy-preserving genotype imputation model utilizes machine learning to predict missing genotypes over an encrypted input, while allowing FHE operations efficiently. Due to the properties of FHE, the genomic data remains encrypted during rest, transit and in use.

Name: Ibrahim Allafi
Supervisor: Lyndon Brown
Area of Research: Robotics and Control

Internal Model Principle-Based Control for Sinusoidal Disturbance Rejection in Field-Oriented Control (FOC)
This research presents results of combining the field-oriented control of motors with a more general Internal Model Principle controller rather than the specific case of integral control. The goal is to have a motor that can remove narrow band disturbances without impacting its performance outside of this specific frequency. This research is motivated by eliminating tremor in human limbs.
We verify our approach by initially implementing the algorithm in Matlab and then conducting experimental trials in our lab using two BLDC motors. The first motor will generate a sinusoidal torque signal on the shaft, while the second motor will utilize our algorithm to cancel this torque. Both motors are connected by a pulley. When Motor one initiates rotation with a sinusoidal torque signal, Motor two driven with our algorithm will freeze the motion in Motor one. Thus, the torque on motor two will match that of motor one. We then add additional broadband torque in Motor one and show that Motor two can still match the sinusoidal torque while ignoring this additional movement. We will investigate the difference between using the encoders from both motors as the driving signal for our control algorithm.

Name: Shamim Mohammadsalehianpirmard
Supervisor: Gerry Moschopoulos
Area of Research: Power Systems

Analysis of a single-phase AC-DC quasi-Z source full-bridge converter
This research investigates the design and analysis of a single-phase AC-DC quasi-Z-source (qZS) full-bridge converter. The AC-DC single-stage converter commonly used in power electronics faces efficiency challenges under low line and heavy load conditions due to its variable intermediate DC bus voltage. In contrast, the Z-source converter (ZSC) offers the ability to both buck and boost the input voltage, with control of the dc-link voltage achieved through direct measurement or by monitoring the capacitor voltage. Quasi-Z-source converters provide a viable solution for applications requiring continuous input current.
The primary objective of this research is to explore the operational modes of quasi-Z-source AC-DC full-bridge converters, particularly the two types of zero-voltage (ZV) states (ZV State #1 and ZV State #2). By studying these modes, the aim is to utilize the ZV states of Z-source converters to maintain a fixed DC bus voltage in a single-stage full-bridge converter. The research methodology involves designing and simulating the proposed converter using MATLAB Simulink, identifying suitable control strategies to vary the ZV states, and achieve the desired energy equilibrium at the DC bus. Simulation results validate the effectiveness of the proposed design in maintaining a fixed DC bus voltage. By adjusting the ZV states in response to load variations, the converter achieves stable voltage output, confirming the theoretical analysis and underscoring the potential of Z-source converters in enhancing the efficiency and performance of power conversion systems.

Name: Patrick Egan
Area of Research:
Supervisor: Ken McIsaac

Adaptive Resonance Theory (ART) is a unique neural network architecture which was proposed by Carpenter, Grossberg and their colleagues in the early 1980's. ART provides its own solution to the "stability-plasticity dilemma", the requirement that a network must be able to balance its ability to learn new patterns while retaining memory of previous patterns. It achieves this with its focus towards achieving "resonance" between an input pattern and one of its learned classes. As with other neural networks, ART is yet another strong candidate for optimization via improved parallel throughput. Graphics Processing Units (GPUs) have become a dominant force with respect to large-scale AI models due to their powerful parallel-processing capabilities. As there are already ART architectures like fuzzy-ART which have been implemented on GPUs, this opens up the possibilities to further enhancing the performance of these networks with GPU optimization techniques.

While there are several publications which already implement ART architectures on GPUs, the majority of them do not consider some GPU optimization techniques such as Kernel Slicing and Kernel Co-scheduling. For many GPU implementations, the application will have low resource occupancy making them more inefficient. Additionally, many of the aforementioned publications about implementing ART models in GPUs do not use high-level models like Directed Acyclic Graphs (DAGs) that help identify bottlenecks and sections of a design which can run in parallel.

This research will be exploring the fuzzy-ART architecture with respect to performance to identify bottlenecks and regions which can reap the benefits of enhanced parallelization. To achieve this, there will be an attempt to develop a DAG of the most optimal path for throughput. With regions that allow for parallel execution identified, it will be possible to experiment with different GPU optimization techniques to improve resource occupancy. Through kernel co-scheduling, it should be possible to observe greater throughput by scheduling kernels which use different resources to execute simultaneously instead of the default "first-in first-out" policy used by more naive approaches.