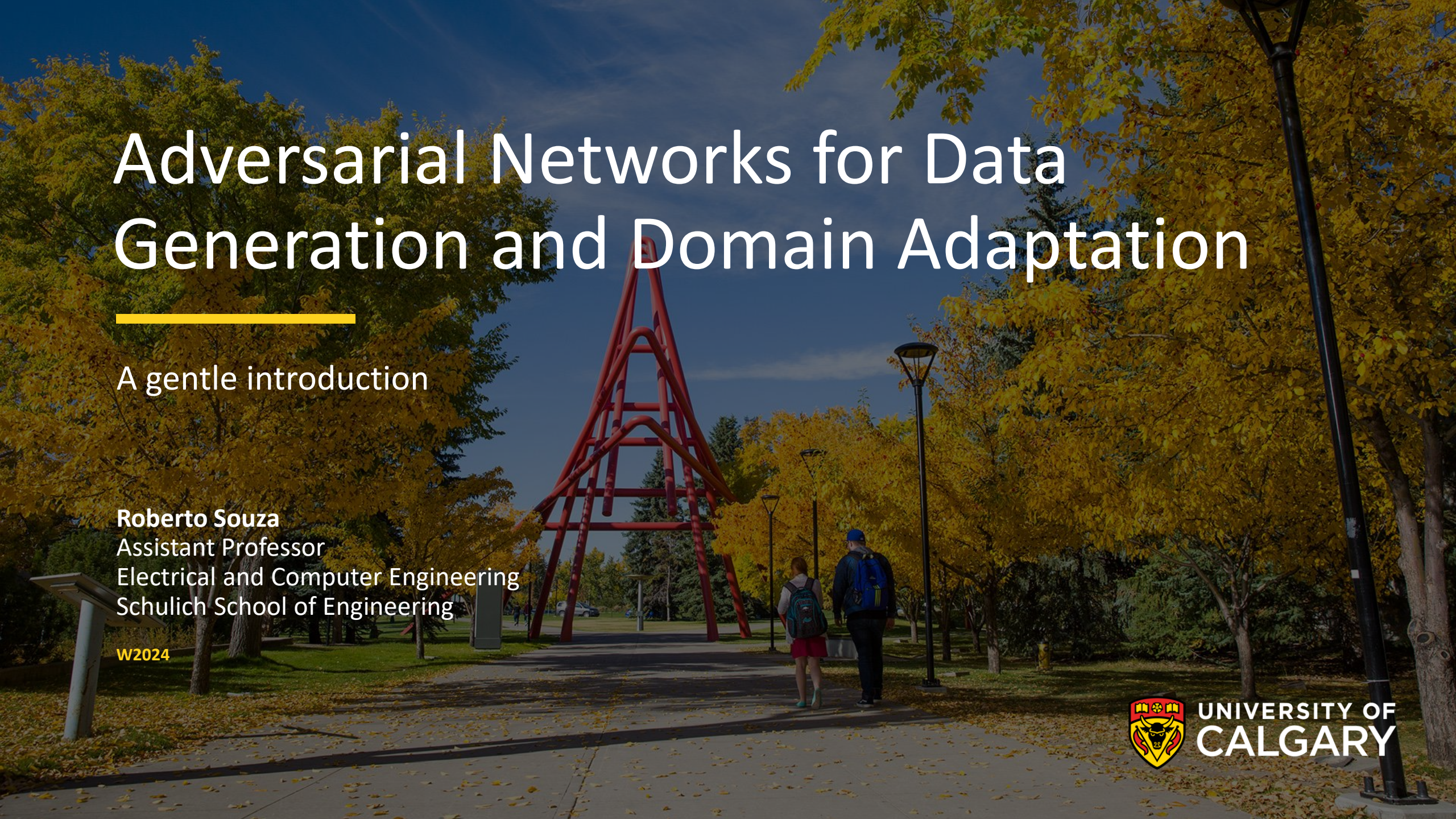


Adversarial Networks for Data Generation and Domain Adaptation

A gentle introduction

Roberto Souza
Assistant Professor
Electrical and Computer Engineering
Schulich School of Engineering

W2024

UNIVERSITY OF CALGARY

Outline

- Learning Goals
- Introduction
- Generative Adversarial Networks (GANs)
- Domain Shift and Domain Adaptation
- Domain Adversarial Neural Networks
- Summary

Learning Goals

- Introduce Generative Adversarial Networks
  - What they do
  - How they work

- Introduce domain shift and domain adaptation concepts
  - Introduce domain adversarial models for domain adaptation

Generative Adversarial Networks (GANs)

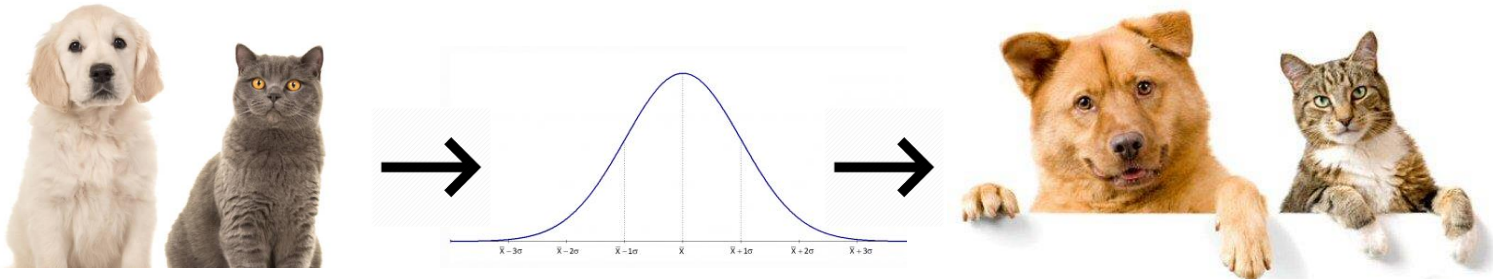
Introduction

- GANs are unsupervised deep learning methods
- GANs are considered one of the greatest deep learning breakthroughs in recent years
- There are many types of GANs
  - Wasserstein GAN
  - Cycle-GAN
- They all operate under the same principle of having modules with adversarial (*i.e.*, competing objectives)

What are GANs?

- GANs are generative models. What is a generative model?
- We have two different models in machine learning:
  - 1) Discriminative models

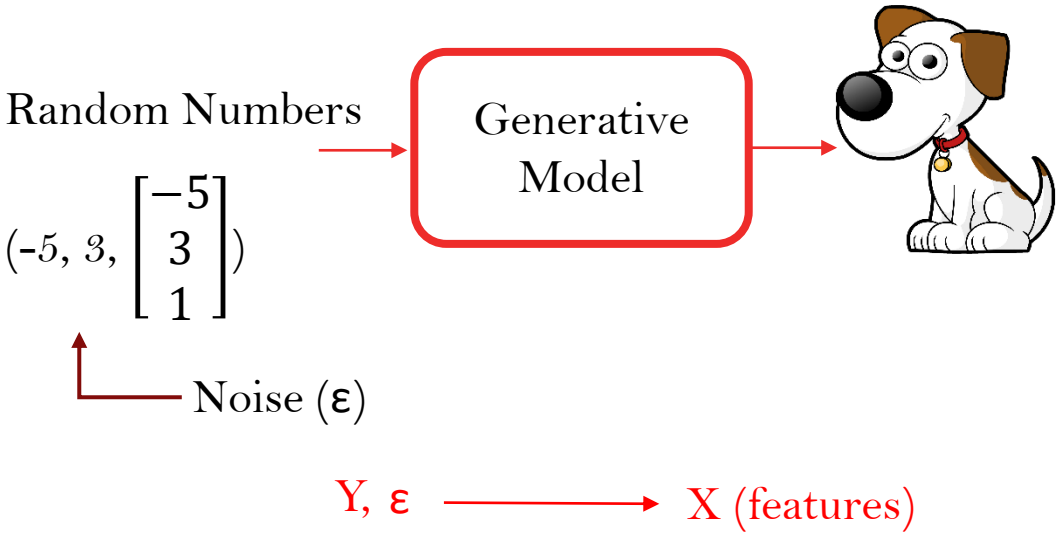
  - 2) Generative models



- Dataset
- Learning distribution
- New data

Machine Learning Models

- Generative Models
  - Generate realistic representation for each class.



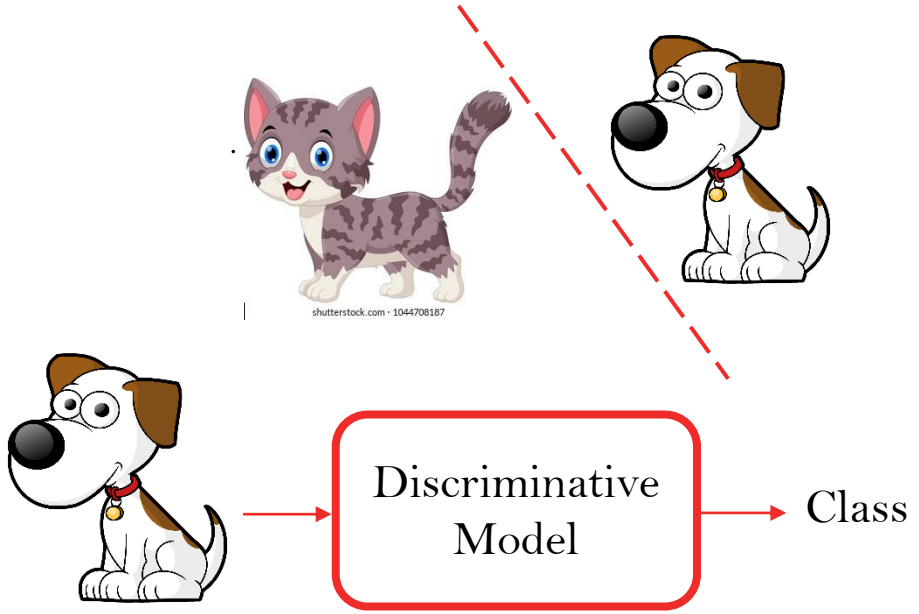
Y, ε → X (features)

$$P(X|Y)$$

or

$$P(X)$$

- Discriminative Models
  - Used for classification problem



X (features) → Y

$$P(Y|X)$$

7

Generative Adversarial Networks

To produce Realistic Presentation of different classes

To distinguish real images from fake ones (produced by generator)

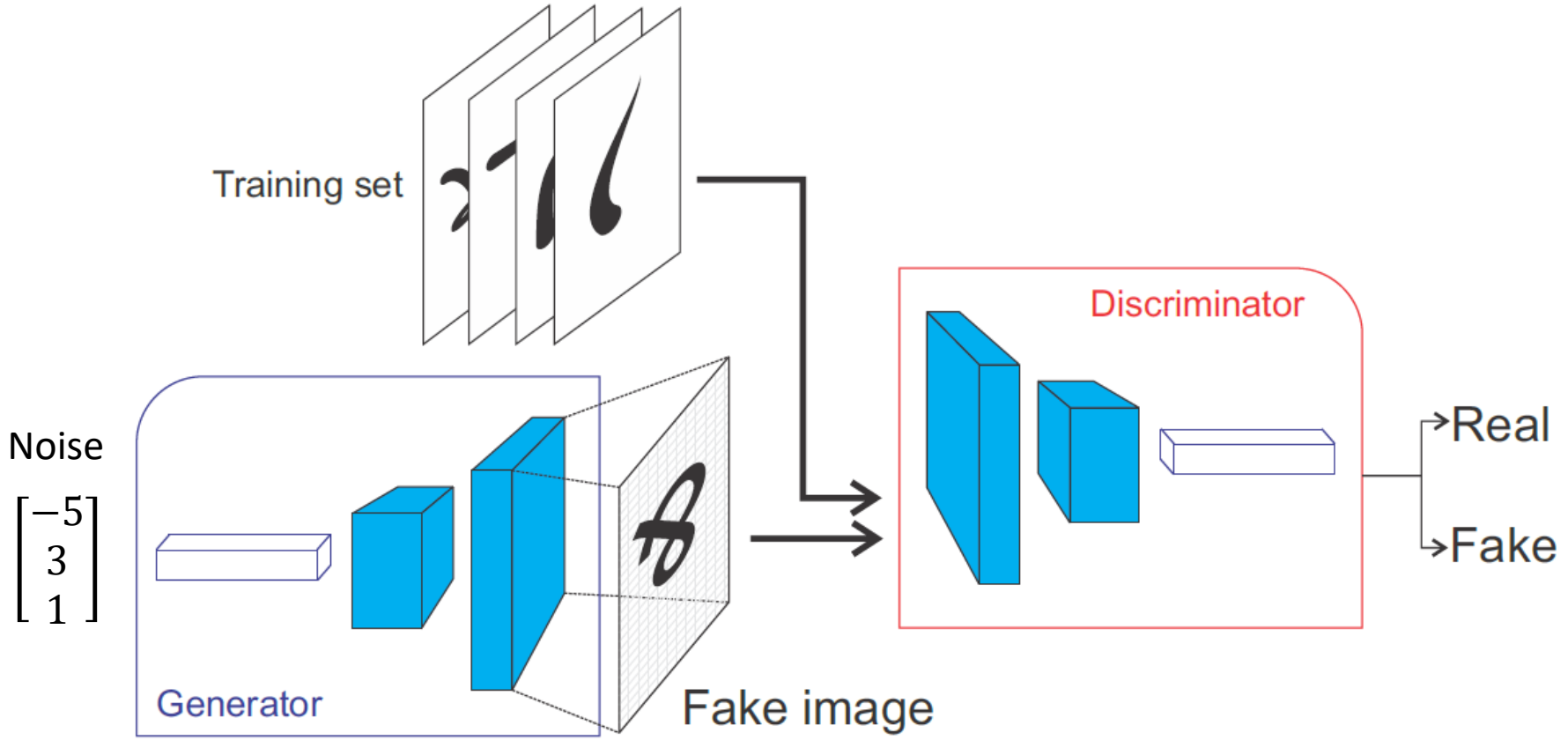
$$\begin{bmatrix} -5 \\ 3 \\ 1 \end{bmatrix}$$ → Generative Model →  → Discriminative Model → Fake/ Real

There is a competition here !

- Generator tries to make fakes that look real and fool the discriminator
- Discriminator learns how to distinguish reals from fakes

GANs are generative models where the data distribution is learned implicitly!

GAN



GANs Problems

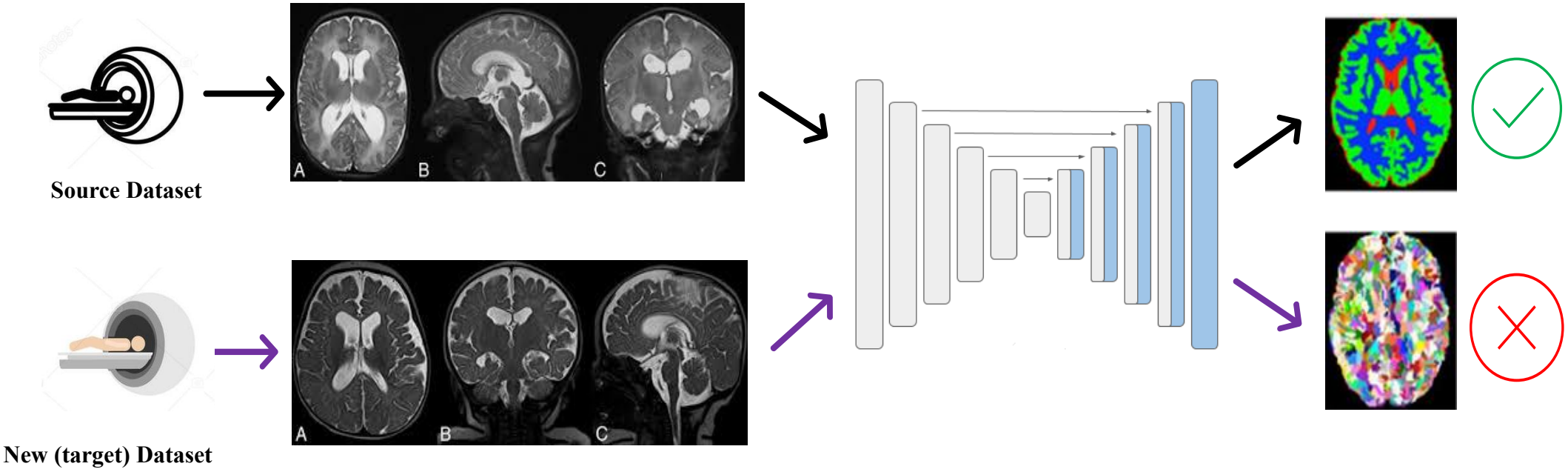
- **Non-convergence**: the model parameters oscillate and the model does not converge
- **Mode collapse**: the generator collapses and produces a limited number of different samples
- **Diminished gradient**: the discriminator is too good that the generator gradient vanishes and learns nothing,
- **Highly sensitive** to the hyperparameter selections.

Summary

- GANs are unsupervised techniques
- They can be used to generate synthetic data that can potentially be used to train other deep learning models
- There are different GAN types, but they are all based on the principle of having two competing objectives
- GANs often face instabilities during training

Domain Shift and Domain Adaptation

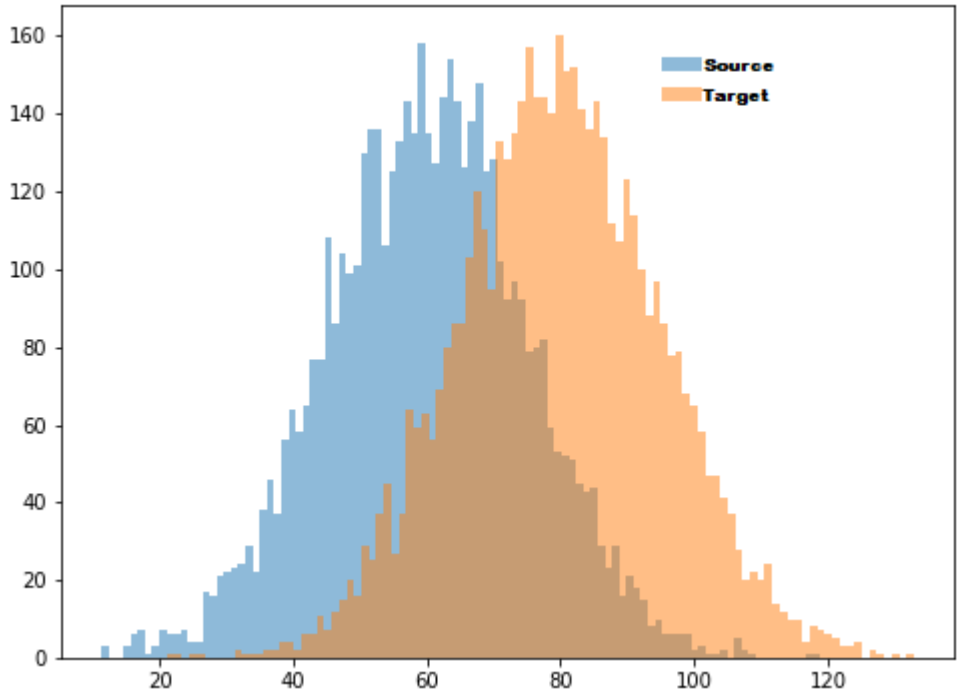
Motivation



Domain Shift

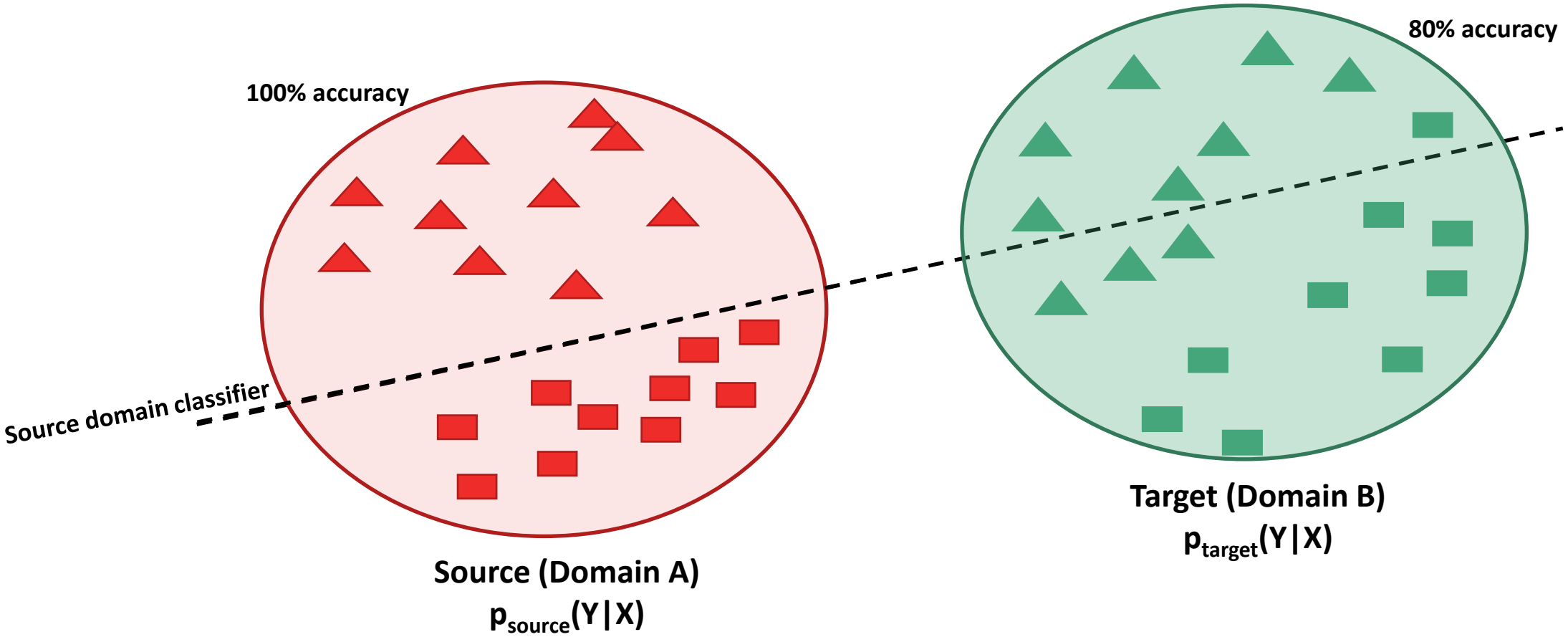
- **Domain shift**: refers to the change of data distribution between one dataset (source/reference domain) and another dataset (target domain).

$$p_{source}(Y|X) \neq p_{target}(Y|X)$$



UNIVERSITY OF CALGARY

Domain Shift Problem

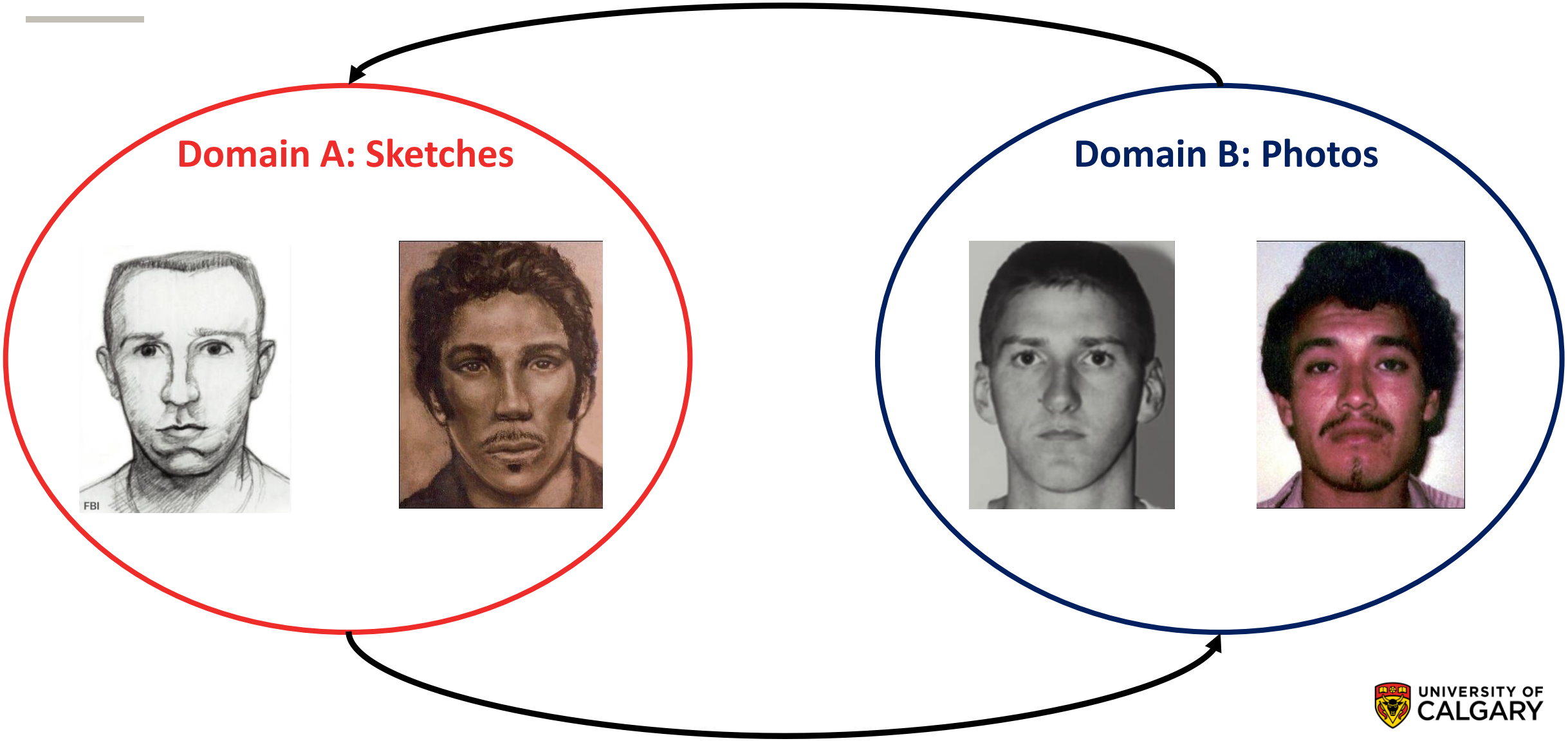


Different Types of Images

Domain A

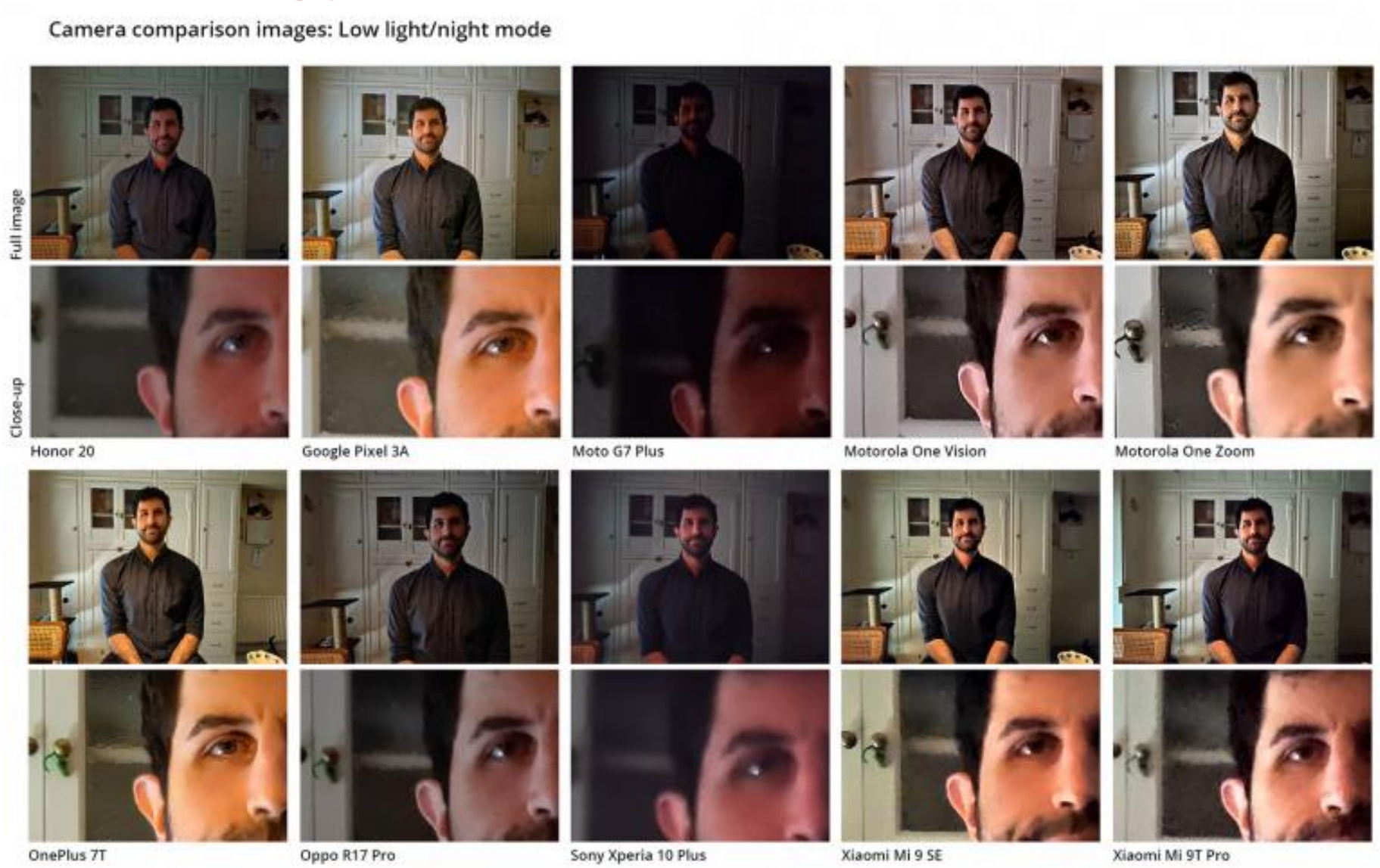
Domain B

Different Types of Images: Sketches and Photos



UNIVERSITY OF CALGARY

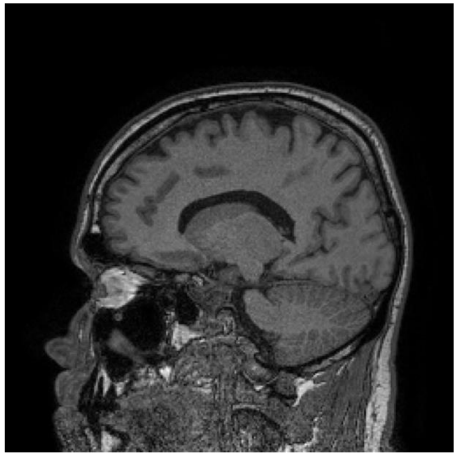
Technology Differences and Evolution



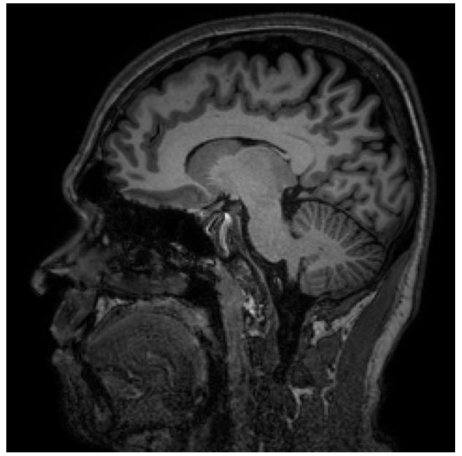
UNIVERSITY OF CALGARY

Hardware and Software Differences

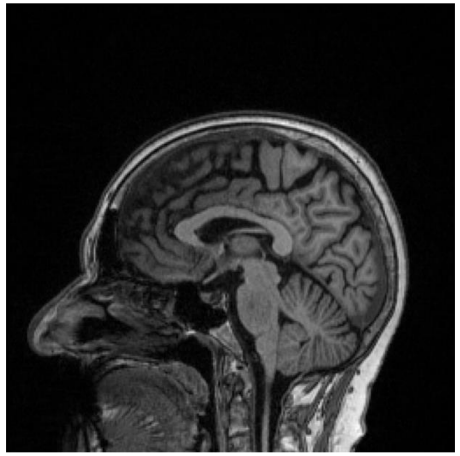
philips_15



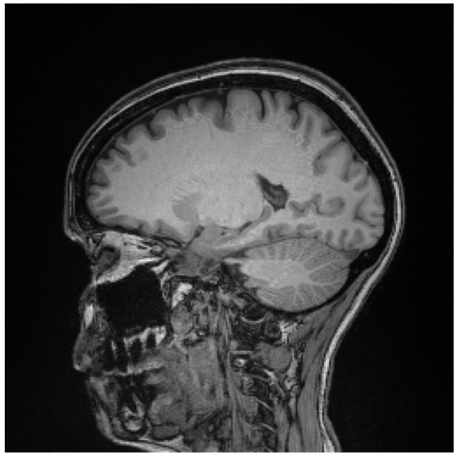
philips_3



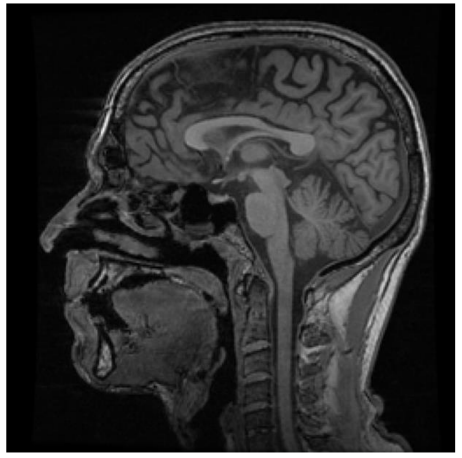
siemens_15



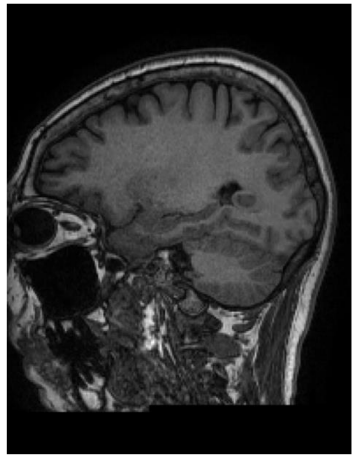
siemens_3

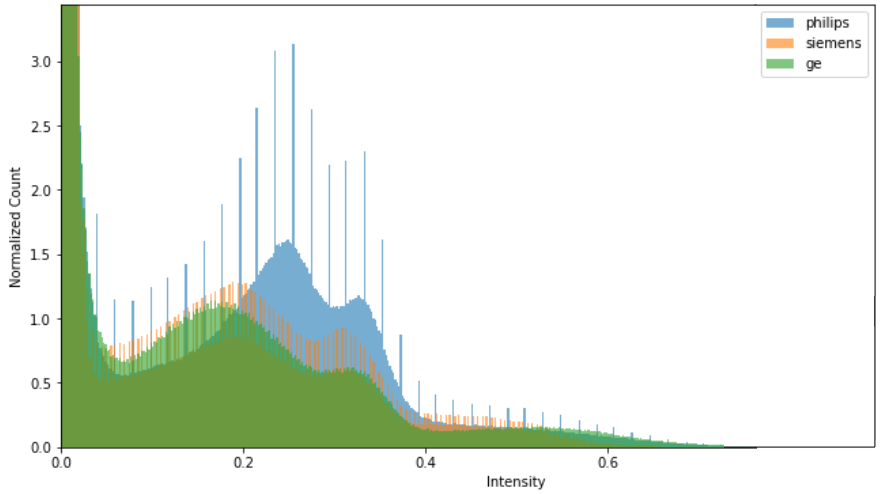


ge_3



ge_15

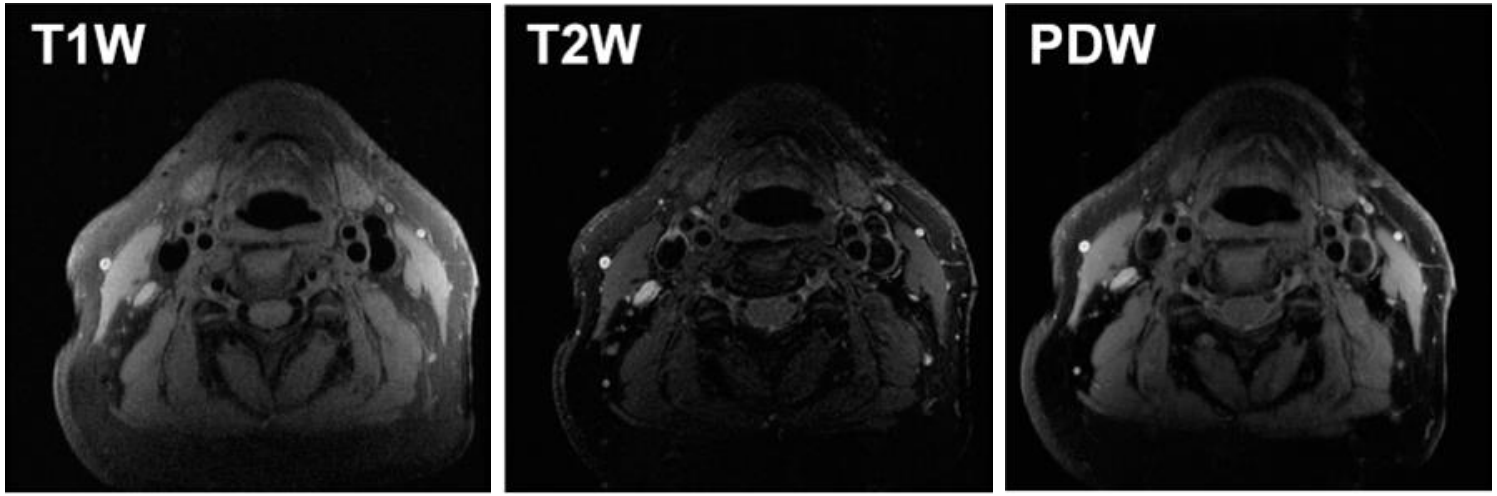




UNIVERSITY OF CALGARY

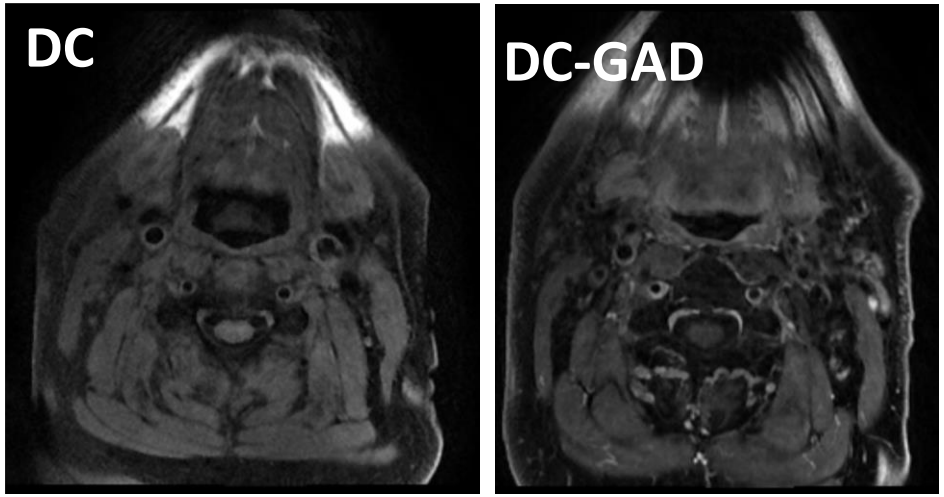
Hardware and Software Differences

AIM-HIGH Study



- The carotid arteries were manually annotated at the time of the study

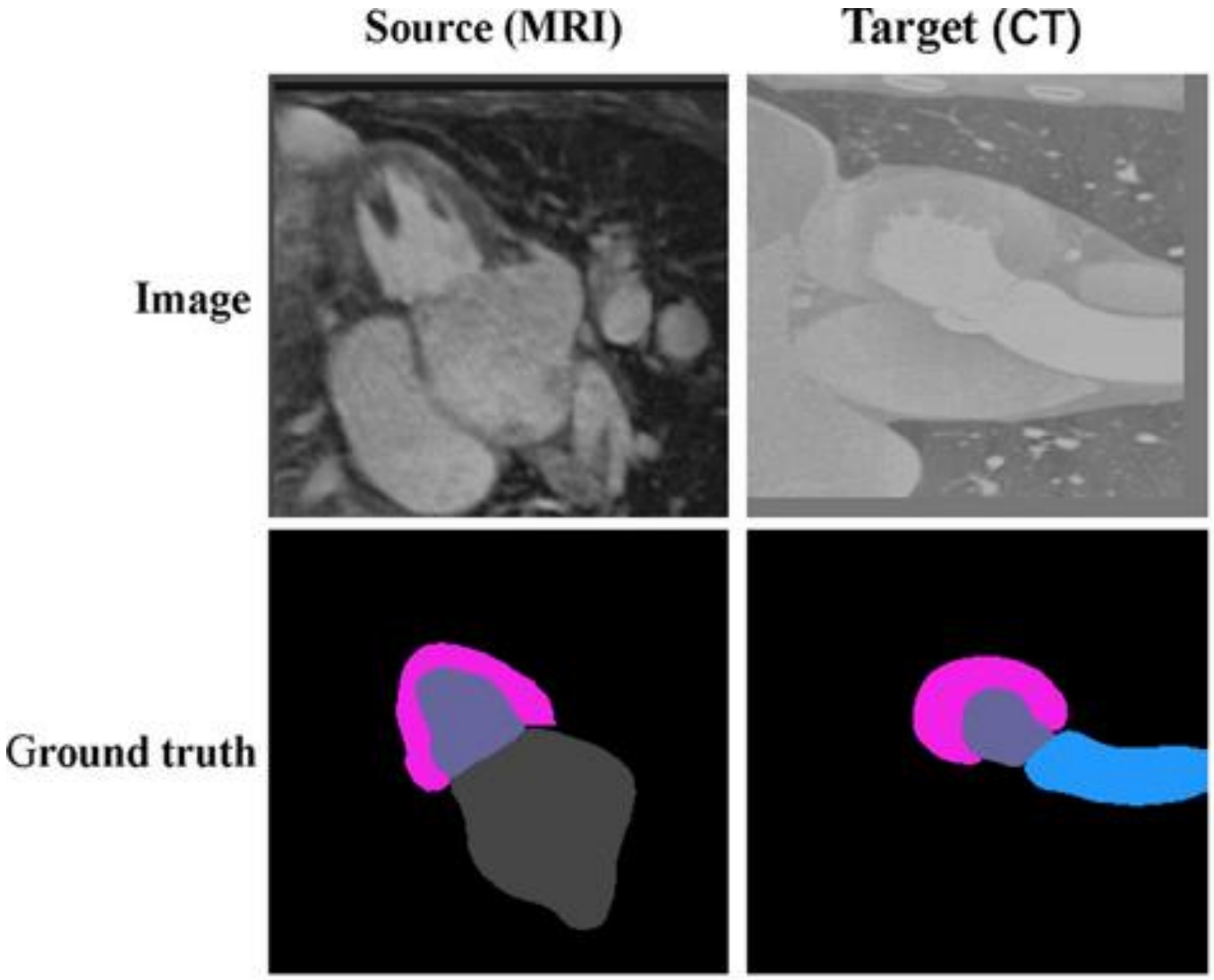
CARDIS Study



- Leverage AIM-HIGH annotated data to create a segmentation model for the data being collected at CARDIS study

UNIVERSITY OF CALGARY

Different Technologies



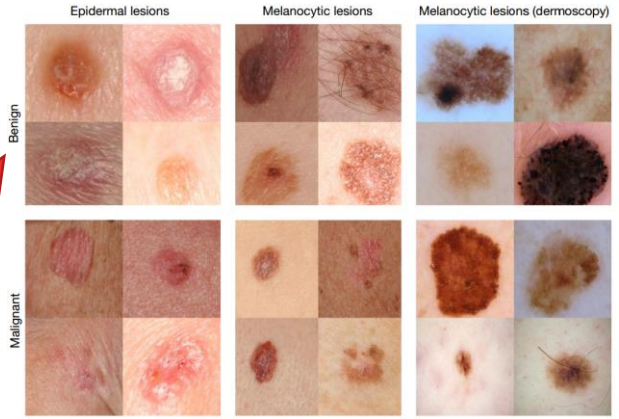
Degree of Domain Shift

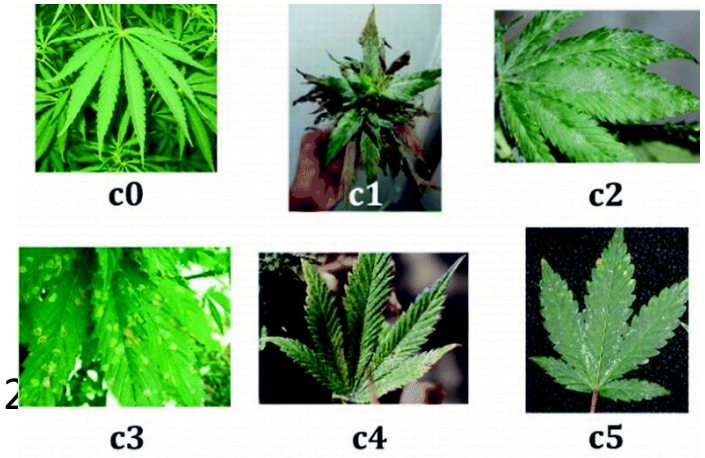
- **Degree of domain shift** is a measure of how much the distributions of the source and target domains are different

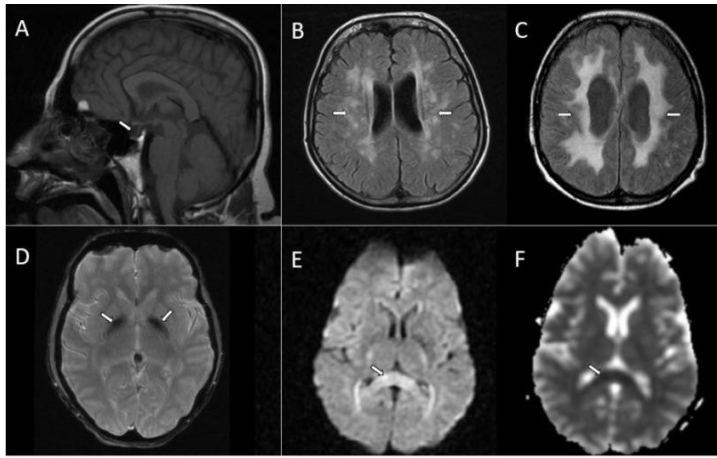
- Previous studies have revealed that the test error generally increases in proportion to the degree of domain shift.

Degree of Domain Shift

Small or large shift?

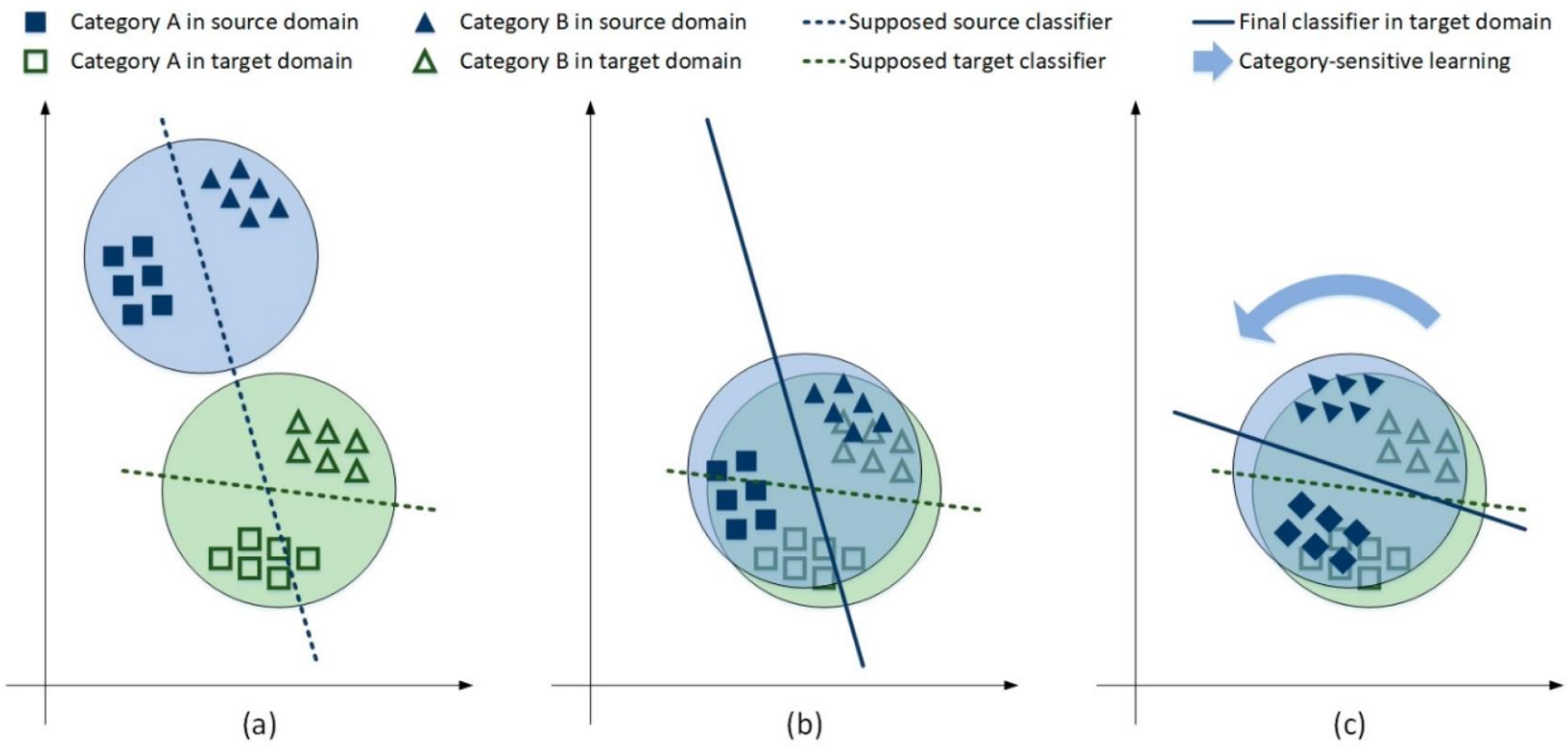




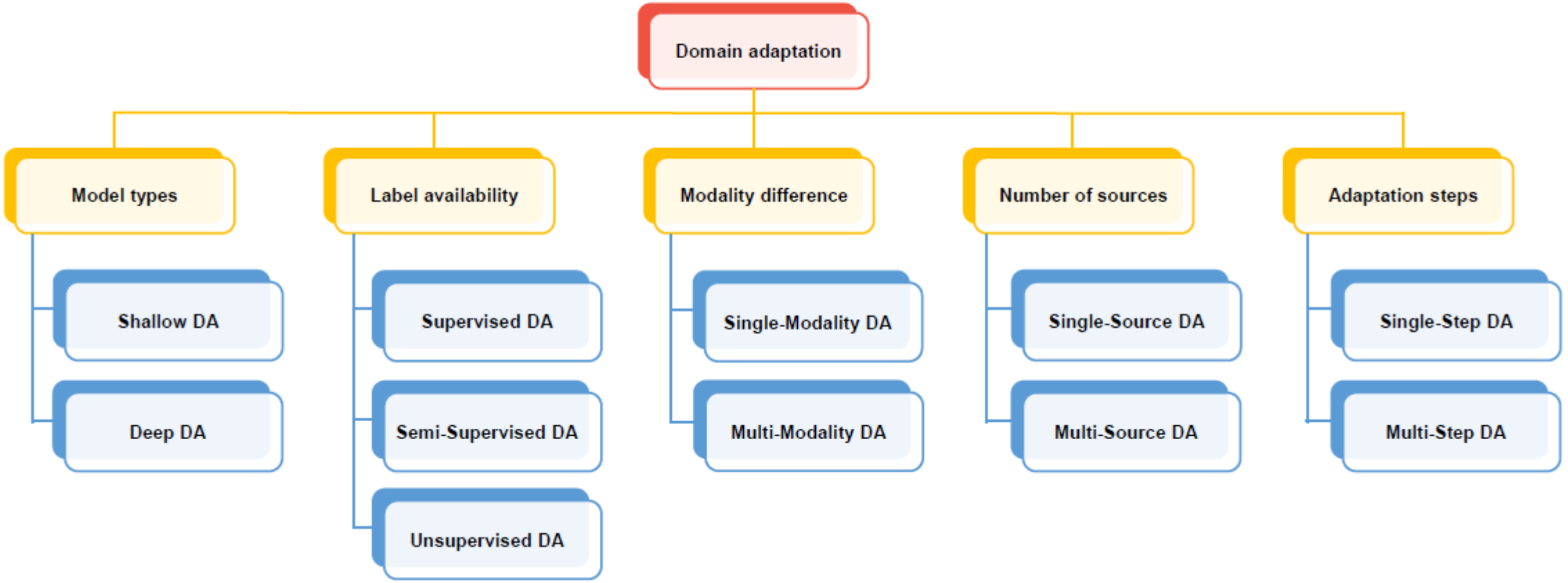


Domain Adaptation

- **Domain adaptation**: domain adaptation refers to adapting a model trained in one or more source domains to a different one or more target domains.



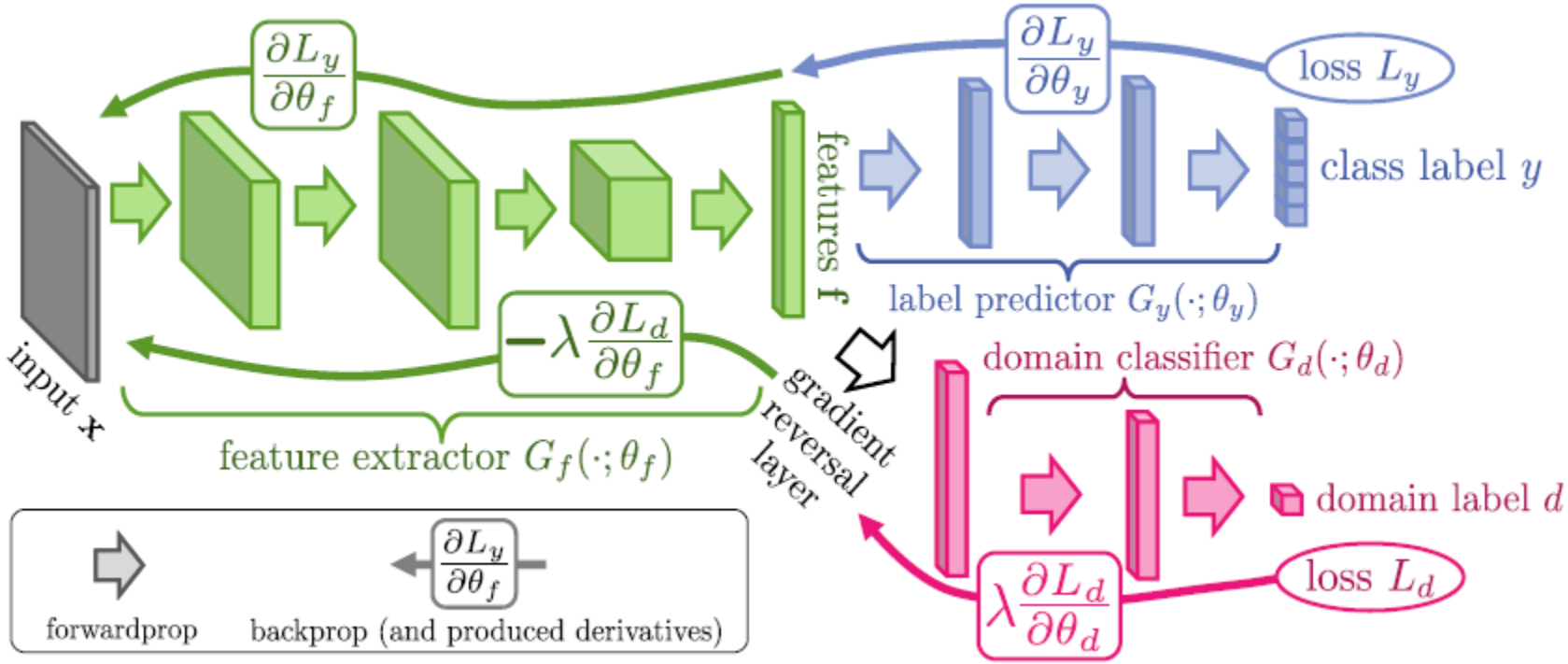
Domain Adaptation Categories



Supervised Domain Adaptation

- Essentially transfer learning
  - Fine-tune all layers
  - Fine-tune initial layers
  - Fine-tune final layers

Domain-Adversarial Training of Neural Networks (Unsupervised)



*Ganin et al., JMLR, 2016

$$E(\theta_f, \theta_y, \theta_d) = \frac{1}{n}\sum_{i=1}^{n}\mathcal{L}_y^i(\theta_f, \theta_y) - \lambda\left(\frac{1}{n}\sum_{i=1}^{n}\mathcal{L}_d^i(\theta_f, \theta_d) + \frac{1}{n'}\sum_{i=n+1}^{N}\mathcal{L}_d^i(\theta_f, \theta_d)\right)$$

Summary

- Domain shift is a problem in machine learning that can make model performance decrease when there is a distribution shift in the test data

- Domain adaptation techniques can be used to make models more robust to data domain shifts

Thank you!