Generative AI (Spring-2025)

Assignment-1

Instructor

Dr. Hajra Waheed PHD

Submission Guidelines:

- Submit your assignment on Google Classroom in the format "20XX.ipynb".
- The deadline is Feb 12, 2025, at 11:59 PM. No extensions will be granted.

Declarations:

- Late submissions will incur penalties: 25% deduction on the first day, 50% on the second day, and zero marks thereafter.
- Plagiarism will result in zero marks for the assignment.
- This is an individual assignment; collaboration or group work is strictly prohibited.
- Please ensure that you submit your own original work.

VIVA Policy:

- A VIVA (oral examination) will be conducted to assess your understanding of the assignment.
- The VIVA will be scheduled separately, and you will be notified of the date and time.
- Failure to attend the VIVA will result in zero marks for the assignment.

Academic Integrity:

- Plagiarism, collusion, and academic dishonesty will not be tolerated.
- Any instances of academic misconduct will be reported to the authorities and may result in severe penalties.

Objective

To implement and compare different Generative AI-based anomaly detection methods in image and signal datasets. The focus will be on leveraging deep learning techniques to generate, reconstruct, and identify anomalies effectively:

1. **Generative Adversarial Networks (GANs)**
2. **Autoencoders (AE) & Variational Autoencoders (VAEs)**

Datasets

We will use the following datasets:

1. **MNIST Digits:** A dataset of handwritten digits (0-9), commonly used for classification and generative models. Contains grayscale images (28×28 pixels).
2. **MNIST Fashion:** A dataset by Zalando, featuring fashion items (e.g., shirts, sneakers, and bags).Consists of grayscale images (28×28 pixels) of 10 different clothing categories.

Part 1: Exploratory Data Analysis (EDA) (5%)

1. **Load the Datasets**
   a. Download and Load the MNIST Digits and MNIST Fashion datasets.
2. **Preview the Datasets**
   a. Display sample images from MNIST Digits and MNIST Fashion to understand their structure.
3. **Dataset Analysis**
   a. Determine the number of samples in each dataset.
   b. Identify the number of classes and their labels in the MNIST Digits and MNIST Fashion datasets.

Part 2: Implementing Generative Adversarial Networks (GANs) (25%)

GAN Model Architecture (35%)

1. Implement a GAN architecture consisting of:
   a. Generator: A neural network that generates fake digit images from random noise.
   b. Discriminator: A neural network that distinguishes between real and fake images.
   c. Adversarial Training: Train both networks in a min-max game to improve generation quality.
2. Train the GAN on MNIST digits and monitor loss curves **(10%)**
3. Train the GAN on MNIST Fashion (Select any 1 class like shoe) and monitor loss curves **(10%)**

Now that your GAN model has been successfully trained, proceed with the following tasks

1. Generate and display **10 newly generated images** from the trained GAN.(5%)
2. Generate and display 5 newly generated images of the digit **"3"** (Replace with the last digit of your roll number: **L238023**) using the trained GAN.(20%)
3. Generate images from fashion dataset like shoe (20%)

Hints:

- **Use a discriminator loss function based on binary cross-entropy:**
- **d_loss = -torch.mean(torch.log(D(real_data)) + torch.log(1 - D(fake_data)))**
- **Train the generator to fool the discriminator:**
- **g_loss = -torch.mean(torch.log(D(G(z))))**

Part 3: Implementing Variational Autoencoder (VAE) (25%)

VAE Model Architecture (35%)

1. Implement a VAE architecture consisting of:
   Encoder: A neural network that compresses input images into a latent vector.
   Reparameterization Trick: Implement the trick to sample from the latent space.
   Decoder: A neural network that reconstructs the images from the latent vector.
2. Train the VAE on the MNIST datasets. **(10+10%)**
3. Extract and visualize the latent space representation using t-SNE/PCA **(5%)**.
4. Generate new digit images by sampling latent vectors and decoding them.

Now that your VAE model has been successfully trained, proceed with the following tasks

1. Implement the function to generate specific digits using stored latent vectors (5%)
2. Generate and display **10 newly generated images** from the trained VAE. (5%)
3. Generate and display 5 newly generated images of the digit **"2"** (Replace with the **second last** digit of your roll number: **L238023**) using the trained GAN. (10%)
4. Generate images from fashion dataset like shoe (20%)

Hint: You may use the following structure to guide your implementation:

- **Encoder: Conv2d ReLU**
- **Decoder: ConvTranspose2d ReLU**
- **Latent Space: Implement reparameterization trick (mu, logvar)**
- **Use the binary cross-entropy (BCE) loss for reconstruction.**
- **Compute KL divergence to regularize the latent space:**
  kl_div = -0.5 * torch.sum(1 + logvar - mu.pow(2) - logvar.exp())

Part 4: Comparison and Analysis (10%)

Compare **GAN vs. VAE** in terms of:

a. **Image Quality:** Which method generates clearer, more realistic digits?
b. **Training Stability:** Which model was harder to train?
c. **Latent Space Representation:** How do GANs and VAEs differ in learning latent spaces?

Discuss potential **improvements** to both models with respect to hyperparameter tuning.

Part 5: Save world with VAE (35%)

Anomaly detection is not just a technical challenge—it's a **financial game-changer**. Across industries, undetected anomalies result in **billions of dollars in losses** each year, from financial fraud and cybersecurity breaches to healthcare misdiagnoses and industrial failures. The ability to **identify rare but high-impact deviations** can lead to **proactive decision-making, cost reduction, and operational efficiency**.

Finance – Fraud costs **$42B+ annually**; VAE flags suspicious transactions, saving banks **millions**.
Cybersecurity – Cybercrime hits **$10.5T by 2025**; AI stops intrusions, cutting breach costs by **$3.58M**.

Healthcare – Misdiagnoses cost **$100B+**, AI reduces errors by **50%**, saving lives & money.
Manufacturing – Downtime losses reach **$50B**; AI-driven maintenance **cuts failures by 40%.**
Retail – Inventory inefficiencies waste **$1.1T**; anomaly detection slashes losses **15–20%.**
Energy – Power failures cost **$150B**; AI detects grid issues, saving **millions**.

The Task is open-ended:

- **Choose a real-world problem** where anomaly detection can drive significant financial savings. Consider areas where anomalies cause massive financial losses, such as **fraudulent transactions in banking, cyberattacks on enterprises, medical misdiagnosis, or equipment failures in industrial settings**.
- **Select a dataset** that reflects real-world challenges, ensuring it contains a mix of normal and anomalous instances. The dataset could come from **finance, healthcare, cybersecurity, industrial IoT, energy, transportation, or any other financially impactful domain**.
- **Implement Variational Autoencoders (VAE)** to detect anomalies. VAEs, a deep generative model, learn the underlying distribution of normal data and flag deviations that indicate anomalies helping businesses **prevent fraud, reduce downtime, and improve operational efficiency**.

Deliverables:

- **Notebook** with code implementations.
- **Detailed Report with screenshot attached (Properly formatted)**.
    - **Handmade Architecture of Models (Neat and well explained)**
    - **Generated images** from both models.
    - **Plots for latent space representation**.
    - **Discussion**