# DETECTION OF FAKE AND REAL AADHAAR CARDS USING CLIP VLM NAME: PRADITA G

Aim: To create a model that can differentiate between real and tampered Aadhaar cards within its dataset which is done by feeding data to the model which helps it classify the features and differentiate accordingly

### PROCEDURE:

### STEP 1:

INPUT AQUSITION: The data set for this classification purpose was created using a base cards template which is Aadhaar like preserving the original structure the logo the slogan their positioning and the font and other styles.

To this base template the other features like name, photo dob, and gender is added.

By tampering the real dataset generated using PIL a Fake dataset for Aadhaar dataset is created

Examples of a few Tampering's applied:

- Name tampering.
- DOB tampering.
- Gender tampering.
- Photo tampering.
- Logo tampering.
- · QR tampering.
- Slogan tampering.
- Xerox/photocopy like tampering
- Noise added.
- Blurring

Progress: Data set creation accomplished.

# STEP 2:

# CLEANING AND ANALYZING THE DATA:

- The data is made free of noise and made better for training.
- We make sure the data is void of white spaces or unnecessary things that can affect the learning capacity of the machine.
- We plot a few graphs or understand the trend of the data before we start training the model to yield better results.

Progress: Data analysis done, and cleaning done data prepared for training

### STEP 3:

# SPLITTING THE DATASET:

- Although this step sounds insignificant splitting the data into parts for training and validation helps for the model to learn better and helps model understanding and evaluate if the model Is an overfitting one or underfitting one from the results of testing with the validation set
- The best way is to split is 80-20 that is 80 percent for training and 20 percent for testing.
- Here I have placed the real photos under a real folder and fake under a fake folder the training and validation have their own pair of real and fake folder with respective images.

# Splitting the data set done

### STEP-4:

# TRAINING THE MODEL:

- The last final and the most crucial step
- We will be using the CLIP a pretrained Vision language model belonging to OPENAI.
- The CLIP pre processer will load the image and process them correctly.
- So, we freeze the layers belonging to CLIP so that during training nothing many changes.
- Only my custom classifier head will be trained every time.
- We have also used focal loss in this case.
- We have used AdamW as the optimizer which is lightly better than Adam.
- We have 15 epochs on whole.
- In each batch we will get CLIP image embeddings
- Pass those embeddings through a custom classifier.
- Compute the focal loss.
- Backpropagate and update the classifier weights.
- Tracks and prints the training loss and accuracy.
- Then we have a validation loop which will switch to evaluation mode and computes the accuracy on validation no weight updates.
- Stores the predicts and labels for later predictions.
- Then at last we will plot the confusion matrix to understand the scenario on what basis the loss and accuracy is being told

Progress: Done!! Training of the model is done and validation of the model's accuracy and confusion as metric is used to check the actual accuracy of the model.

Picture of the Aadhaar template:



# CODE SNIPPET FOR REAL CARD GENERATION:

```
card = Image.open(template_path).copy()
draw = ImageDraw.Draw(card)
w, h = card.size
font_hindi_scaled = ImageFont.truetype(font_hindi_path, int(base_font_size * scale))
font_english_scaled = ImageFont.truetype(font_english_path, int(base_font_size * scale))
font_dob_scaled = ImageFont.truetype(font_dob_path, int((base_font_size - 3) * scale))
font_aadhaar_scaled = ImageFont.truetype(font_aadhaar_path, int((base_font_size + 6) * scale))  # Aadhaar number bigger
name_english, name_hindi, gender = random.choice(name_mapping)
aadhaar_number = random_aadhaar_number()
dob = random_dob()
user_photo = get_random_photo(gender)
photo_left = int(w * 0.055)
photo_top = int(h * 0.27)
photo_width = 192
photo_height = 210
 card.paste(user_photo, (photo_left, photo_top))
y_start = photo_top + 5
line_spacing = int(h * 0.085)
qr_left = int(w * 0.8)
 aadhaar\_text\_bbox = draw.textbbox((\emptyset, \emptyset), aadhaar\_number, font=font\_aadhaar\_scaled) \\ aadhaar\_text\_width = aadhaar\_text\_bbox[2] - aadhaar\_text\_bbox[0] \\ aadhaar\_text\_height = aadhaar\_text\_bbox[3] - aadhaar\_text\_bbox[1] \\ 
available_space_left = photo_left + photo_width + 10
available_space_right = qr_left - 10
available_space_width = available_space_right - available_space_left
aadhaar\_x = available\_space\_left + (available\_space\_width - aadhaar\_text\_width) \ // \ 2 - 5 \\ aadhaar\_y = int(h * 0.75)
draw.text((x_right_of_photo, y_start), name_hindi, font=font_hindi_scaled, fill=(0, 0, 0))
draw.text((x_right_of_photo, y_start + line_spacing), name_english, font=font_english_scaled, fill=(0, 0, 0))
draw.text((x_right_of_photo, y_start + 2 * line_spacing), f"008: {dob}", font=font_english_scaled, fill=(0, 0, 0))
draw.text((x_right_of_photo, y_start + 3 * line_spacing), f"Gender: {gender}", font=font_english_scaled, fill=(0, 0, 0))
draw.text((aadhaar_x, aadhaar_y), aadhaar_number, font=font_aadhaar_scaled, fill=(30, 30, 30))
\label{linear_card_1} output\_path = os.path.join(output\_folder, f"aadhaar\_card\_\{1\}.png") \\ card.save(output\_path)
print(f" Saved {output_path}")
```

# **EXAMPLE OF REAL CARDS:**







### **EXPLANATION:**

- This Python script generates **100 fake Aadhaar card images** using a given Aadhaar card template.
- It randomly selects names (in English and Hindi) and gender from a predefined list, generates a random Aadhaar number in the XXXX XXXX XXXX format, and creates a random date of birth (DD/MM/YYYY).
- For each card, it picks a photo from separate male and female photo folders, resizes it to fit the Aadhaar layout, and pastes it onto the template.
- It then writes the name, date of birth, gender, and Aadhaar number onto the card using appropriate fonts (for Hindi and English text)
- This script is useful for creating sample datasets or testing Aadhaar-related software.

### CODE SNIPPET FOR FAKE CARDS CREATION BY TAMPERING OF REAL DATASET:

```
fake adhaar dataset.py >.
     from PIL import Image, ImageDraw, ImageFont, ImageFilter, ImageOps
   template_path = r"D:\empty1.png"
output_folder = "tampered_aadhaar_cards"
   male_photo_folder = r"males"
   female_photo_folder = r"females"
    font_hindi_path = "Noto_Sans_Devanagari/static/NotoSansDevanagari-Regular.ttf"
    font_english_path = "arial.ttf"
    font dob path = "arial.ttf"
    font_aadhaar_path = "courbd.ttf"
    base_font_size = 22
    os.makedirs(output_folder, exist_ok=True)
          e_mapping = [
("Amit Sharma", "अमित शर्मा", "Male"),
("Ravi Patel", "रित पटेल", "Male"),
("Sita Verma", "सीता तर्मा", "Female"),
("Rahul Gupta", "राहुल गुप्ता", "Male"),
("Pooja Reddy", "पुजा रेड्डी", "Female"),
("Vijay Mishra", "तिजय HAYM", "Male"),
("Neha Yadav", "नेहा यातव", "Female"),
("Anjali Singh", "अंजिल सिंह", "Female"),
("Geepak Kumar", "दीपक कुमार", "Male"),
("Kavita Joshi", "किता जोशी", "Female")
    def random_aadhaar_number():
           """Generate random Aadhaar number."""
return " ".join(["".join([str(random.randint(0, 9)) for _ in range(4)]) for _ in range(3)])
                'Generate random date of birth.""
           return f"{random.randint(1, 28):02d}/{random.randint(1, 12):02d}/{random.randint(1965, 2000)}"
```

```
def change color band(card):
        Change color band to random color."""
    draw = ImageDraw.Draw(card)
    band_area = (0, int(card.height * 0.15), card.width, int(card.height * 0.22))
    random_color = tuple(random.choices(range(256), k=3))
    draw.rectangle(band_area, fill=random_color)
    return card
def apply_blur(card):
    return card.filter(ImageFilter.GaussianBlur(radius=2))
def apply_xerox_effect(card):
        Apply xerox (black & white and blur) effect only to base card, not text."""
    base_card = card.convert("L") # Convert to grayscale
base_card = base_card.filter(ImageFilter.GaussianBlur(radius=1))
    return base card.convert("RGB") # Convert back to RGB for drawing text later
for i in range(1, 101):
    card = Image.open(template_path).copy()
    draw = ImageDraw.Draw(card)
    scale = w / 600
font_hindi_scaled = ImageFont.truetype(font_hindi_path, int(base_font_size * scale))
    font_english_scaled = ImageFont.truetype(font_english_path, int(base_font_size * scale))
font_dob_scaled = ImageFont.truetype(font_dob_path, int((base_font_size - 3) * scale))
    font_aadhaar_scaled = ImageFont.truetype(font_aadhaar_path, int((base_font_size + 6) * scale)
    # Pick original detail:
    name_english, name_hindi, gender = random.choice(name_mapping)
    aadhaar_number = random_aadhaar_number()
    dob = random dob()
    user_photo = get_random_photo(gender)
    # Insert photo
photo_left, photo_top = int(w * 0.055), int(h * 0.27)
    card.paste(user_photo, (photo_left, photo_top))
    # Apply tampering based on batch
    if batch == 1: # Name tampering
    fake_name_english, fake_name_hindi, _ = tamper_name(gender)
        name_english = fake_name_english
        name_hindi = fake_name_hindi
    elif batch == 2: # Xerox
        card = apply_xerox_effect(card)
    elif batch == 3:
        card = apply_blur(card)
        gender = tamper_gender(gender)
```

```
def random_dob():
    """Generate random date of birth,"""
    return *f*(random.randint(1, 28):02d)/(random.randint(1, 12):02d)/{random.randint(1965, 2000)}"

def get_random_photo(gender):
    """Get random_photo based on gender.""
    folder = male_photo.folder if gender == "Male" else female_photo_folder
    photo = lists = so.listsdirfolder)
    random_photo = random.choice(photo_list)
    photo = lange.open(os.path.join(folder, random_photo)).convert("RGB")
    photo = photo.resize((192, 210), Image.LANCZOS)
    return photo

def tamper_name(original_gender):
    """Replace original name with a random fake name (gender matched).""
    filtered_fake.names = [f for f in fake.name.mapping if f[2] == original_gender]
    return random.choice(filtered_fake.names)

def tamper_gender(original_gender == "Male" else "Male"

def tamper_gender(original_gender == "Male" else "Male"

def tamper_logo(card):
    """Remove logo from Aadhaar card.""
    draw = imageDow.Draw(card)
    logo_area = (int(card.width * 0.05), int(card.height * 0.05), int(card.width * 0.25), int(card.height * 0.15))
    draw.rectangle(logo_area, fill=(255, 255, 255))
    return card

def tamper_slogan(card):
    """Remove slogan from Aadhaar card.""
    draw = mamgeDow.Draw(card)
    slogan_area = (int(card.width * 0.3), int(card.height * 0.9), int(card.width * 0.7), int(card.height * 0.95))
    draw.rectangle(slogan_area, fill=(255, 255, 255))
    return card

def tamper_slogan(card):
    ""Remove or distort OR code.""
    draw = (int(card.width * 0.7), int(card.height * 0.05), int(card.width * 0.95), int(card.height * 0.05), int(card.width * 0.95), int(card.height * 0.25))
    if random.choice([frine, false]):
    draw.rectangle(qraea, fill=(255, 255, 255))
    else:
    shad noise
    for _in range(1800);
    for _in range(1800);
    draw.reatangle(qraea, fill=(255, 255, 255))
    cles:
    shad noise
    for _in range(1800);
    draw.reatangle(qraea, fill=(255, 255, 255))
    return card
```

### **EXAMPLE OF FAKE CARDS:**







# **EXPLANATION OF THE CODE SNIPPET:**

- This Python script generates **100 tampered Aadhaar card images** for testing and simulation purposes using the **Pillow (PIL)** library.
- It starts with a base template and overlays randomized user details like name (in English and Hindi), gender, date of birth, Aadhaar number, and a photograph selected based on gender.
- The script applies different tampering techniques across batches such as name and gender mismatches, QR code distortion, logo/slogan removal, color band changes, blur effects, and xerox-like black-and-white simulation to create realistic variations.
- Each card is saved in a specified output folder with sequential filenames for easy organization. This tool is ideal for creating synthetic datasets for training tamper-detection systems or testing document verification algorithms.

## SPLITTING OF THE DATASET:

```
🕏 splitting.py > ...
      original_real_dir = "generated_aadhaar_cards"
original_fake_dir = "tampered_aadhaar_cards"
      base_dir = "dataset"
      for split in ["train", "validation"]:
   for cls in ["real", "fake"]:
               split_dir = os.path.join(base_dir, split, cls)
               os.makedirs(split_dir, exist_ok=True)
      train_ratio = 0.8
      def split_and_copy(src_dir, dst_train_dir, dst_val_dir):
          images = os.listdir(src_dir)
           random.shuffle(images)
           train_count = int(len(images) * train_ratio)
           for img in images[:train_count]:
                src_path = os.path.join(src_dir, img)
               dst_path = os.path.join(dst_train_dir, img)
               shutil.copy2(src_path, dst_path)
           for img in images[train_count:]:
                src_path = os.path.join(src_dir, img)
               dst_path = os.path.join(dst_val_dir, img)
               shutil.copy2(src_path, dst_path)
      split_and_copy(
          original_real_dir,
          os.path.join(base_dir, "train", "real"),
os.path.join(base_dir, "validation", "real")
       split_and_copy(
          original_fake_dir,
           os.path.join(base_dir, "train", "fake"),
os.path.join(base_dir, "validation", "fake")
      print(" Done splitting dataset!")
```

Here we have successfully split the dataset into training and validation.

80-20

### TRAINING CODE SNIPPET:

```
train_dataset = CLIPDataset(train_dir, clip_processor)

train_dataset = CLIPDataset(val_dir, clip_processor)

train_dataset = CLIPDataset(val_dir, clip_processor)

### Fix class immalance

labels = label for __label in train_dataset.dataset.samples]

class_counts = torch.bincount(troch.tensor(tabels))

class_counts = torch.bincount(troch.tensor(tabels))

class_weights = l. / class_weights[label] for label in labels]

sampler = torch.utils_data.Detaloader(train_dataset, batch_size.patch_size, sampler-sampler)

val_loader = torch.utils_data.Dataloader(val_dataset, batch_size.patch_size, shuffle=False)

print(f* Class weights: (class_weights)*)

#### Focal toss to handle imbalance

class focalloss (m.houle):

#### Focal toss to handle imbalance

class focalloss (m.houle):

#### super(focalloss, self).__init__()

### self_agamma = gamma

### self_require(in = reduction

### self_agamma = gamma

### self_require(in = reduction)

### self_require(in =
```

```
optimizer.zero_grad()
                    optimizer.step()
                   running_loss += loss.item()
                    _, predicted = torch.max(outputs, 1)
correct += (predicted == labels).sum().item()
                   total += labels.size(0)
              print(f" Epoch [{epoch+1}/{epochs}], Loss: {running_loss/len(train_loader):.4f}, Train Acc: {train_acc:.2f}*")
             # Validation
classifier.eval()
             val_correct, val_total = 0, 0
all_preds, all_labels = [], []
                 for images, labels in val_loader:
   images, labels = images.to(device), labels.to(device)
   image_features = clip_model.get_image_features(pixel_values=images)
                         outputs = classifier(image_features)
_, predicted = torch.max(outputs, 1)
                         val_correct += (predicted == labels).sum().item()
val_total += labels.size(0)
                         all_preds.extend(predicted.cpu().numpy())
                         all_labels.extend(labels.cpu().numpy())
             val_acc = 100 * val_correct / val_total
print(f" Validation Acc: {val_acc:.2f}%")
                 best_val_acc = val_acc
                         'clip_model_state_dict': clip_model.state_dict(),
'classifier_state_dict': classifier.state_dict()
                   }, "best_model.pth")
print(" Best model saved!")
        # Classification report
print("\n Final Classification Report:")
        print(classification_report(all_labels, all_preds, target_names=train_dataset.dataset.classes))
        cm = confusion_matrix(all_labels, all_preds)
148
        sns.heatmap(cm, annot=True, fmt="d", cmap="Blues",
xticklabels=train_dataset.dataset.classes,
```

```
plt.title("Confusion Matrix")
plt.xlabel("Predicted")
plt.ylabel("Actual")
plt.show()
```

# OUTPUT:

(.venv) PS D:\codings\machine_learning\open_cv> python trainings.py
Using device: cpu
Using a slow image processor as `use_fast` is unset and a slow processor was saved with this model. `use_fast=True` will be the default behavior in v4.52, even
to use a slow processor with `use fast=False`.
Class weights: tensor([0.0101, 0.0093])
Epoch 1/15: 190% 26/26 [00:26<00:90, 1.92s/it]
Epoch [1/15], Loss: 0.1746, Train Acc: 56.04%
Validation Acc: 56.78%
Best model saved!
Epoch 2/15: 100% 26/26 [00:26<00:00, 1.02s/it]
Epoch [2/15], Loss: 0.1649, Train Acc: 59.90%
Validation Acc: 65.25%
Best model saved!
Epoch 3/15: 100% 26/26 [00:25<00:00, 1.02it/s]
Epoch [3/15], Loss: 0.1586, Train Acc: 65.70%
Validation Acc: 48.31%
Epoch 4/15: 100% 26/26 [00:26<00:90, 1.02s/it]
Epoch [4/15], Loss: 0.1543, Train Acc: 64.25%
Validation Acc: 57.63%
Epoch 5/15: 100% 26/26 [00:20<00:00, 1.27it/s]
Epoch [5/15], Loss: 0.1565, Train Acc: 67.15%
Validation Acc: 73.73%
Best model saved!
Epoch 6/15: 109% 26/26 [00:27<00:00, 1.06s/it]
Epoch [6/15], Loss: 0.1484, Train Acc: 69.08%
Validation Acc: 58.47%
Epoch 7/15: 100% 26/26 [00:22<00:00, 1.16it/s]
Epoch [7/15], Loss: 0.1457, Train Acc: 70.05%
Validation Acc: 83.05%
Best model saved!
Epoch 8/15: 100% 26/26 [00:21<00:00, 1.21it/s]
Epoch [8/15], Loss: 0.1323, Train Acc: 83.09%
Validation Acc: 90.68%
Best model saved!
Epoch 9/15: 100% 26/26 [00:20<00:00, 1.26it/s]
Epoch [9/15], Loss: 0.1269, Train Acc: 83.57%
Validation Acc: 85.59%
Epoch 10/15: 100% 26/26 [00:21<00:00, 1.24it/s]
Epoch [10/15], Loss: 0.1287, Train Acc: 77.29%
Validation Acc: 58.47%
Epoch 11/15: 100% 26/26 [00:19<00:00, 1.31it/s]
Epoch [11/15], Loss: 0.1309, Train Acc: 78.74%
Validation Acc: 89.83%
Epoch 12/15: 100% 26/26 [00:17<00:00, 1.49it/s]
Epoch [12/15], Loss: 0.1227, Train Acc: 77.78%
Validation Acc: 79.66%
Epoch 13/15: 109% 26/26 [00:17<00:00, 1.51it/s]
Epoch [13/15], Loss: 0.1141, Train Acc: 79.23%
Validation Acc: 92.37%
Best model saved!
Epoch 14/15: 109% 26/26 [00:16<00:00, 1.58it/s]
Epoch [14/15], Loss: 0.1085, Train Acc: 83.09%
Validation Acc: 83,05%
Epoch 15/15: 100% 26/26 [00:18<00:00, 1.39it/s]
Epoch [15/15], Loss: 0.1043, Train Acc: 88.41%
Validation Acc: 88.98%
·

Final Classification Report:						
	precision	recall	f1-score	support		
fake	0.92	0.83	0.87	54		
real	0.87	0.94	0.90	64		
accuracy			0.89			
	precision	recall	f1-score	support		
fake						
real	0.87	0.94	0.90	64		
			0.00	110		
accuracy			0.89	118		
fake	0.92	0.83	0.87	54		
real				64		
1 Cui	0.07	0.54	0.50	•		
accuracy			0.89	118		
accuracy			0.89	118		
accuracy			0.89	118		
macro avg	0.89	0.89	0.89	118		
weighted avg	0.89	0.89	0.89	118		

FINAL ACCURRACY OF THE MODEL: 90%