Advanced Machine Learning

Final Project

Fingerprint Generation with Diffusion Models

💡 Aryan Tiwari (B20AI056)
Ayush Abrol (B20AI052)
Udit Agarwal (B20ME076)

Introduction

Diffusion models represent a class of mathematical and computational models used in various fields to describe the spread of information, diseases, innovations, or any phenomena that propagate through a medium over time or space. These models are commonly used in fields such as epidemiology, sociology, economics, physics, and more.

Fingerprint diffusion models can replicate the unique patterns found in fingerprints by simulating the movement of particles within a medium, mimicking the ridges, valleys, and minutiae characteristic of individual fingerprints. They incorporate mathematical algorithms that simulate the diffusion process, allowing for the creation of synthetic fingerprints with high fidelity to real-world patterns.

Dataset

The Synthetic Fingerprint Database (SOCOFing) is a widely used dataset for fingerprint recognition research. It contains synthetic fingerprint images generated with custom software, providing a diverse set of fingerprint patterns and minutiae configurations.

• The real data contains 6000 fingerprints for 600 subjects as every subject has 10 fingerprints that represent the five fingers on every hand -

• The altered data is the same data with some augmentation.

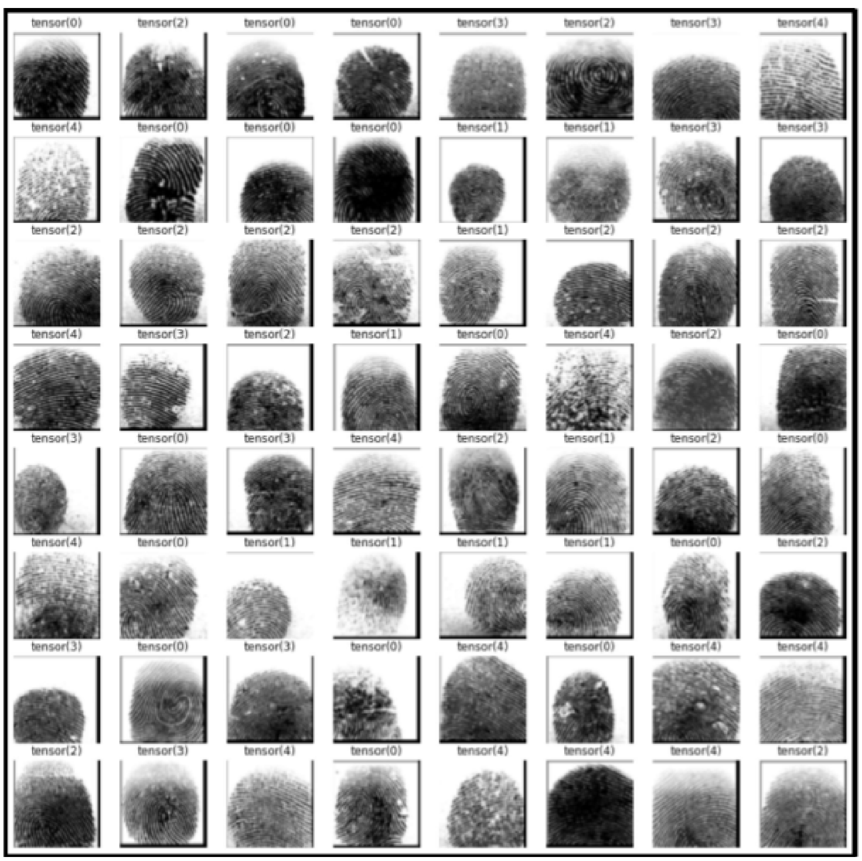
• There are three different versions of the altered data: easy-medium-hard .

• The augmentation of the data is: obliteration, central rotation, and z-cut .

• The names for every photo is in format [(subject index)(gender)_(finger_name).BMP]

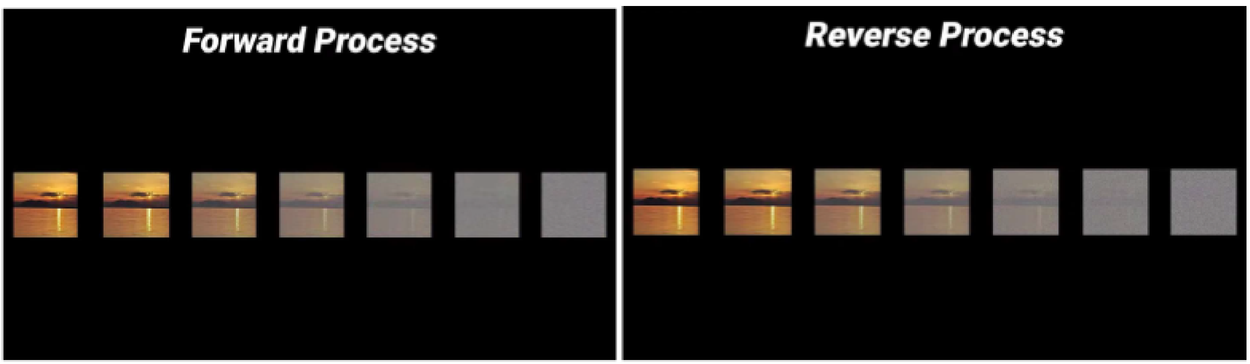
The finger names with their corresponding labels are:

1. index_finger -> 0
2. little_finger -> 1
3. middle_finger -=> 2
4. ring_ finger -> 3
5. thumb_finger --> 4



We are using images of (3x64x64), we ave converted these single channel images to 3-channel images.

Methodology



Left to Right Right to Left

We have written code that defines two classes, "UNet" and "UNet_conditional", which represent variations of the U-Net architecture tailored for different purposes.

Overview and explanation of the code:

"UNet" class is an implementation of a U-Net model for image processing tasks. It consists of an encoder-decoder structure and employs self-attention mechanisms at different levels.

1. Components
   • Encoder (Down): Contains downsampling blocks to capture higher-level features.
   • Self-Attention (SelfAttention): Incorporated at various levels to enable the model to attend to different parts of the input.
   • Bottleneck Layers (DoubleConv): Central layers that process the deepest features.
   • Decoder (Up): Contains upsampling blocks to recover spatial information.

2. Methods
   • "pos_encoding": Function to create positional encodings for time dimensions used within the attention mechanism. *
   • "forward": Performs the forward pass through the U-Net model, applying operations at each level of the architecture.

The "UNet_conditional" class extends the functionality of the "UNet" by introducing conditional inputs to the model. It includes an embedding layer for conditioning the network on specific labels.

1. Changes:
   • Label Embedding (abel_emb): Allows conditioning the model on a specific number of classes, enhancing the network's adaptability for different label inputs.
2. Additional Parameters:
   • "num_classes": A specified number of classes for conditional embedding.
   • Conditioning in "forward": Incorporates label information (if provided) into the positional encoding, altering the input representation based on the provided labels.

The code defines the architecture for the U-Net-based model designed for image processing tasks, possibly suitable for tasks such as image generation. The "UNet_conditional" class extends the basic "UNet" by incorporating conditional information such as which finger to generate in our case (index, middle, ring, little, thumb)

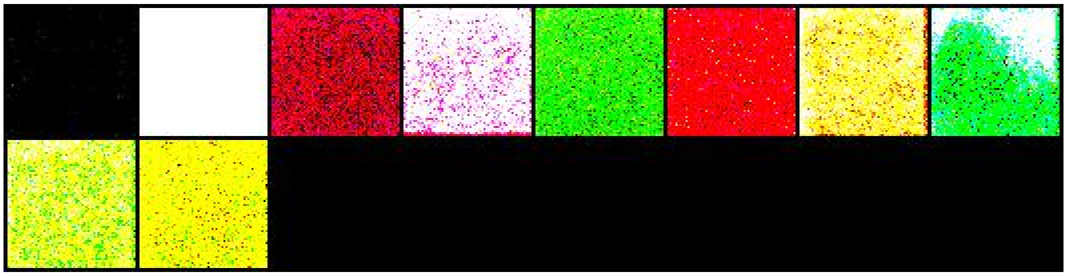
Implementation

To utilize these classes, we have:

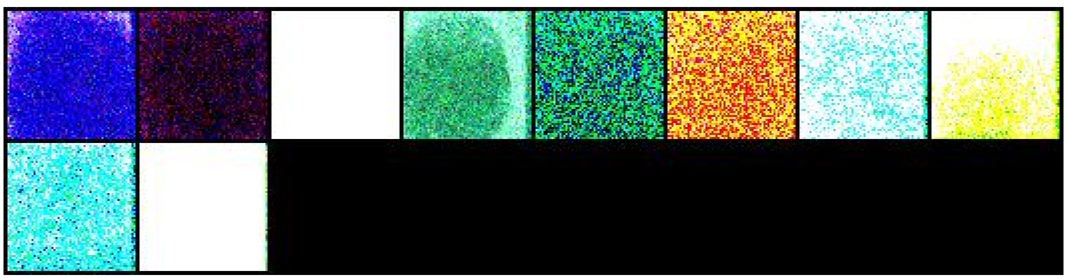
- Prepared data for the model, ensuring it matches the input requirements. We have adjusted the SOCOfing data in the order expected by-torch.data.Dataloader class.
- Initialized the model instance by instantiating "UNet_conditional" with appropriate parameters.
- Train the model using MSE loss functions and AdamW optimizer.
- Use the model for image generation.

Results

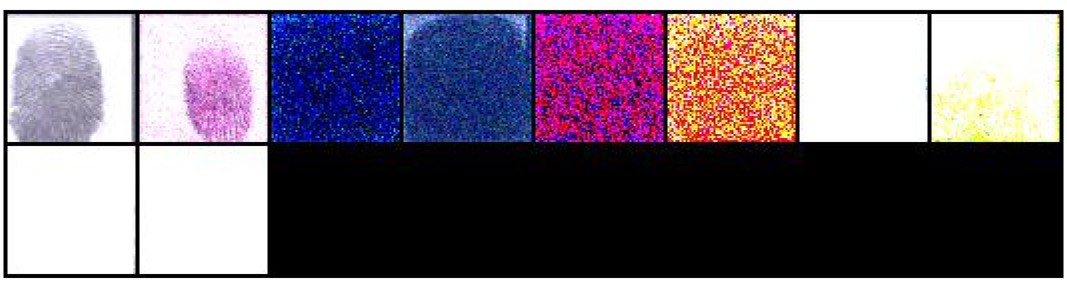
- Epoch 0:



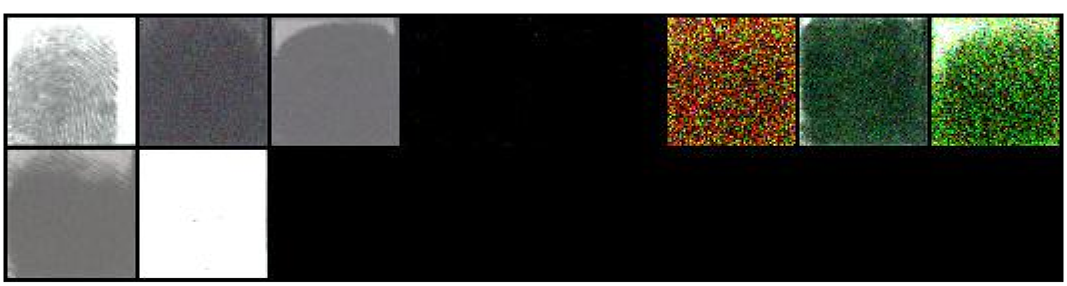
- Epoch 10:



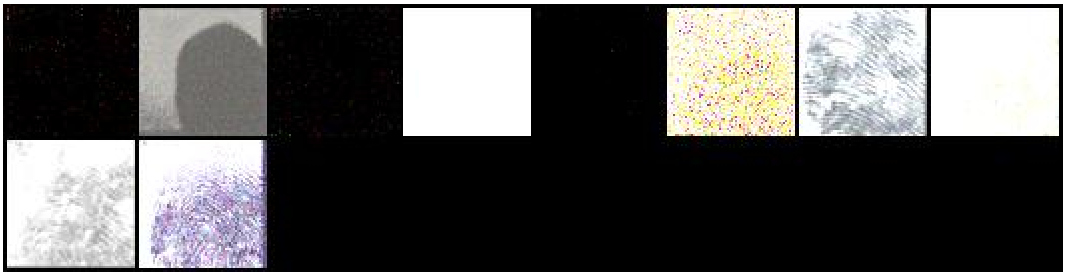
- Epoch 20:



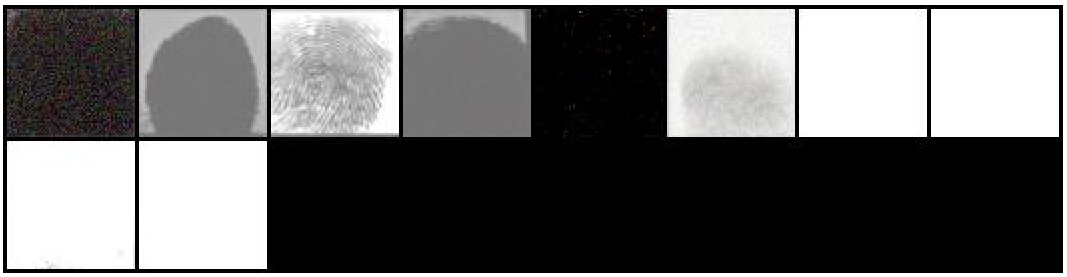
- Epoch 30:



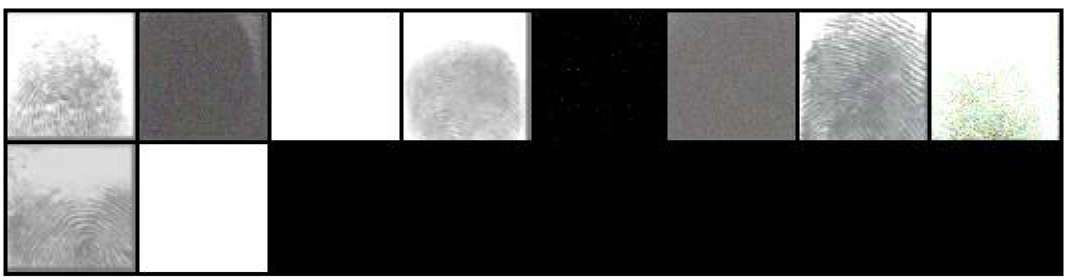
- Epoch 40:



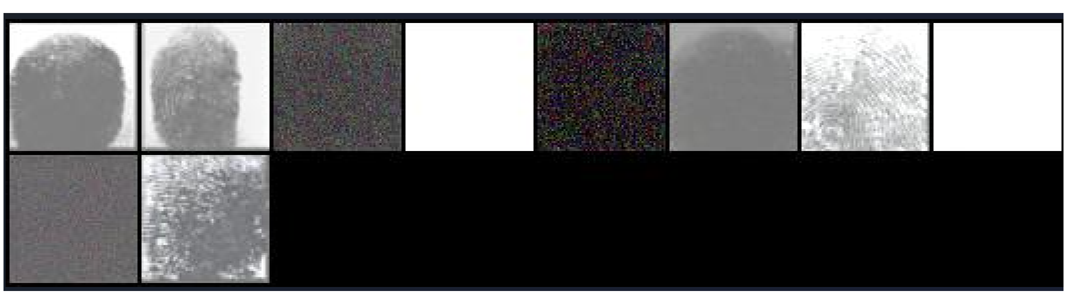
- Epoch 50:



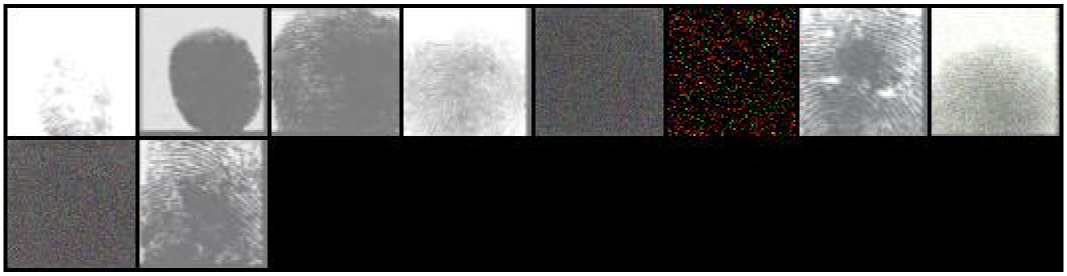
- Epoch 60:



- Epoch 70:



- Epoch 80:



Conclusion

In conclusion, the utilization of diffusion models in generating fingerprints has yielded significant success, particularly evident in the application of 80 epochs on the Synthetic Fingerprint Database (SOCOFing). Through this approach, we have successfully replicated intricate fingerprint patterns and structures that closely resemble those found in actual fingerprints.

The synthesis of fingerprints via diffusion models, particularly on a comprehensive database like SOCOFing, showcases the potential for generating highly realistic and intricate fingerprint images. This accomplishment holds immense promise for various fields, including biometrics, forensic science, and security systems.

The ability to simulate fingerprints with such accuracy and fidelity contributes significantly to advancing fingerprint recognition technology. These synthetic fingerprints serve as invaluable resources for the development, refinement, and rigorous testing of fingerprint identification algorithms. Moreover, they facilitate the evaluation and enhancement of security measures relying on biometric authentication.

The success achieved through the application of diffusion models on the SOCOFing database underscores the effectiveness and versatility of this approach. It not only aids in generating lifelike fingerprint images but also deepens our understanding of the underlying principles governing fingerprint formation and deformation.

Ultimately, this milestone signifies a substantial leap forward in the realm of biometrics and security, paving the way for more reliable and sophisticated fingerprint recognition systems, thereby enhancing security measures across various domains.

Thank You