**"Morph Detect: An AI-driven Solution for Detecting Biometric Face Morphing Attacks on Synthetic Images"**

**Authors:** Yashwanth Balan Arumugam & Pragya Avinash Mishra

**"Morph Detect: An AI-driven Solution for Detecting Biometric Face Morphing Attacks on Synthetic Images"** is a project that proposes an AI-based solution to detect biometric face morphing attacks on synthetic images. Biometric face morphing is a technique used by attackers to combine two different faces into a single synthetic image to bypass face recognition systems. The proposed solution uses a deep convolutional neural network to identify the characteristic features of a face, and then compares these features between two images to detect any morphing. The researchers trained and evaluated the model on a large dataset of real and synthetic images, achieving high accuracy in detecting morphing attacks. The proposed solution has the potential to improve the security of face recognition systems by identifying and preventing biometric face morphing attacks.

The selected subject of detecting face morphing attacks is important because it addresses a significant threat in the digital age. Face morphing attacks involve the creation of synthetic images by blending two or more faces together to create a new face that appears real. These synthetic images can be used for malicious purposes, such as identity theft, fraud, and impersonation. As a result, there is a critical need for effective techniques to detect and prevent face morphing attacks. Deep learning techniques, such as MixFaceNet, have shown promising results in detecting these attacks, highlighting the importance of continued research and development in this area.

MixFaceNet has shown superior performance in detecting face morphing attacks compared to other popular image classification networks such as VGG16 and ResNet50. MixFaceNet is a lightweight network, making it computationally efficient and faster than larger networks. The use of MixFaceNet can improve the security of biometric authentication systems and prevent fraudulent access. Another benefit of deep learning is its ability to learn and adapt to new data. This means that the performance of the model can be improved over time by training it with more data. Additionally, deep learning models can be optimized for different hardware platforms, which can result in faster and more efficient processing.

However, there are also some challenges and drawbacks associated with this technology. One challenge is that deep learning models require a large amount of data for training, which can be time-consuming and costly. Furthermore, the accuracy of the model can be affected by the quality and diversity of the training data, as well as the choice of network architecture and hyperparameters.

The reliance on deep learning models like MixFaceNet can potentially lead to biases and inaccuracies in the results, particularly when the training data is biased or incomplete. MixFaceNet's reliance on large amounts of data and computing power can be a significant barrier for smaller organizations or those with limited resources. Another potential drawback of deep learning for detecting face morphing attacks is that it may not be able to detect more sophisticated attacks that use advanced techniques such as adversarial attacks.