赋能边端协同　　让AI无处不在

英特尔人工智能创新应用大赛

一起联想AI PC

EncryptFace

Face Encryption Recognition System

Based On Generative Model

参赛类别：个人赛道

指导教师：董兴波

项目负责人：田信

项目成员：田信 张慧 杨跃浙 王立稳 吕兴国

2023年12月16日-2024年5月11日

主办方：英特尔中国开源技术委员会、英特尔大湾区科技创新中心

大赛独家AI PC合作伙伴：Lenovo 联想

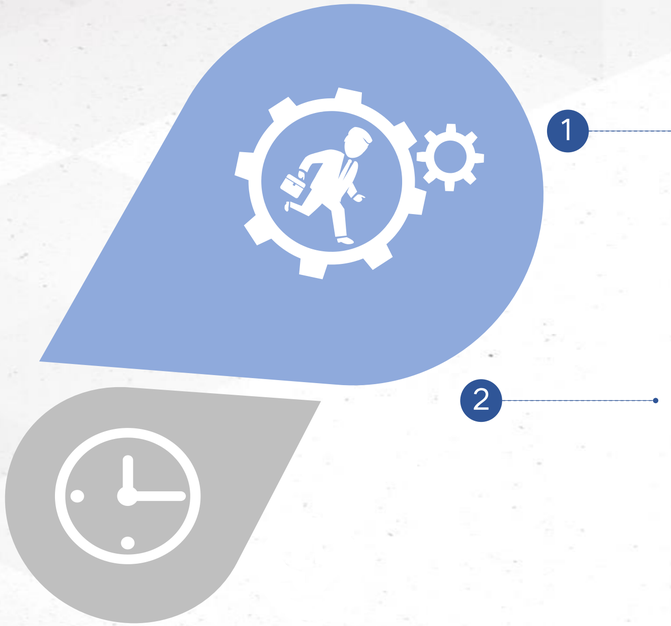
方案简介

Creative theme

Our scheme uses a reversible encryption algorithm to realize the function of face derecognition and recovery recognition. The encrypted encoding is generated by converting the face image into the encoding of the latent space and then processing the encoding and cryptography using Diffusion Model. In the decryption phase, the original face image can be recovered by entering the correct password; if the wrong password is entered, a new de-identified face image with photo fidelity is generated.

方案简介

Highlights of the scheme



1. The face image is encrypted and stored in a database and only decrypted for identification during authentication.

2. This is a two-factor authentication that combines a face and a password. Only the user can match the corresponding original face image if the user provides the correct face information and password.

3. This is the first attempt to use the diffusion model in a two-factor authentication system to protect user privacy. It provides more efficient, flexible, and diverse privacy protection solutions.

方案简介

Highlights of the scheme

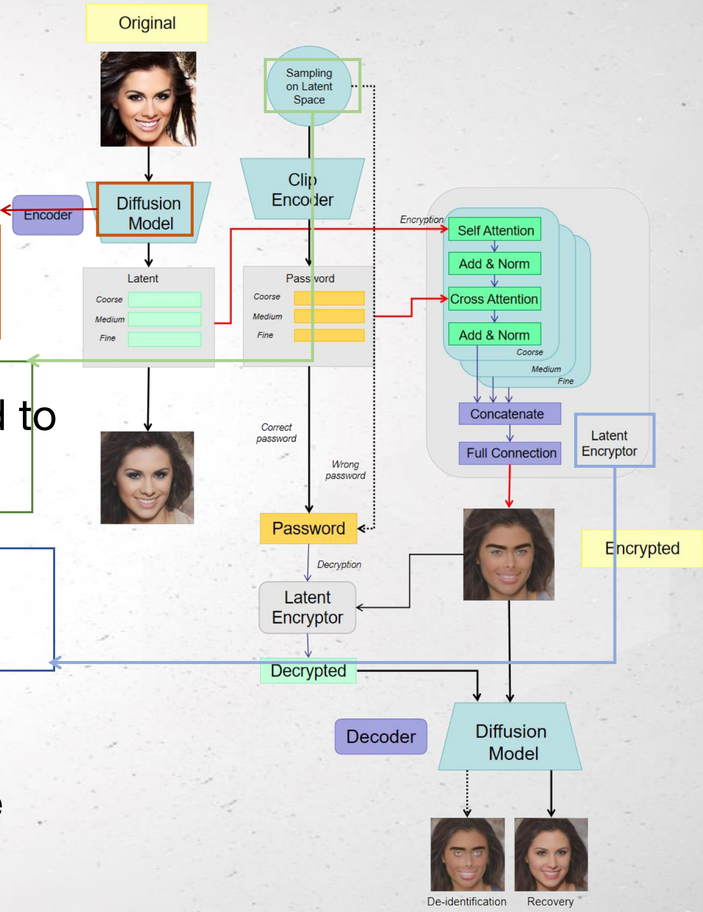
The scheme does not require prior design of complex encryption rules, nor additional condition information or preserved face image sets, and can be trained and applied in an end-to-end manner.

1. The original images were reverse mapped to latent space through a series of noise adding steps.

2.Combined with the password, the denoising process can be controlled to encrypt the latent representation of the image.

3. Responsible for using the password to further encrypt the sampled potential vector.

4. The diffusion model generator will start with the encrypted latent representation, gradually remove the added noise, and generate the de-identified image

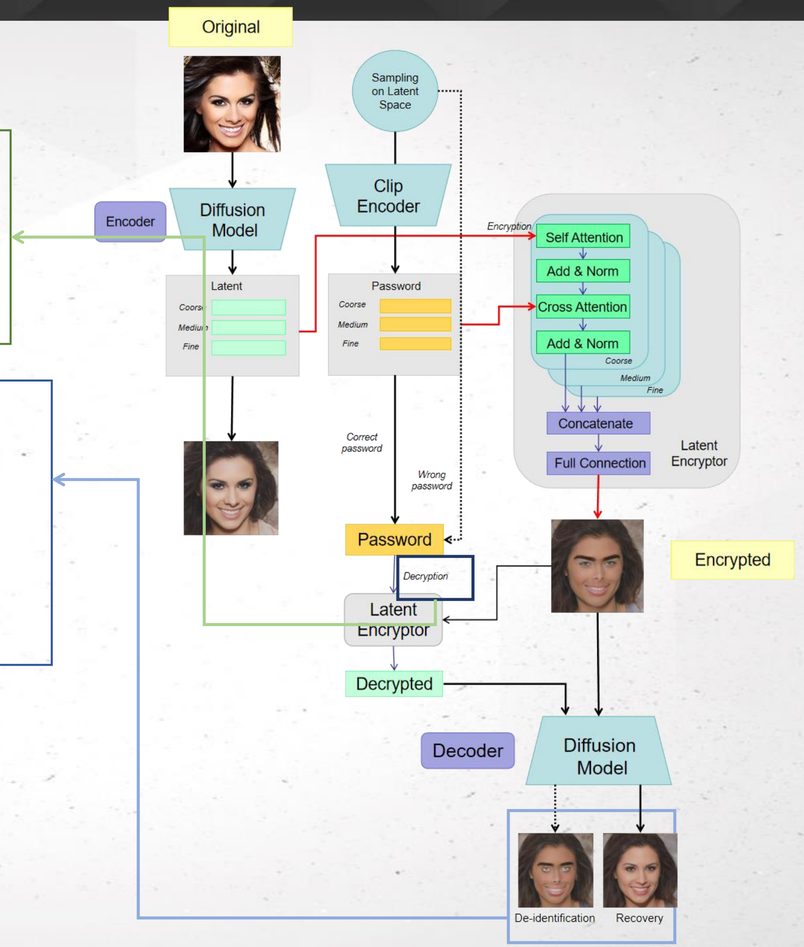


方案简介

Highlights of the scheme

5.The diffusion model generator will start with the encrypted latent representation, gradually remove the added noise, and generate the de-identified image

6. An encrypted latent vector is used to generate an image without personally identifiable information. The recovery process is to use the correct password to convert the encrypted potential vector into the original potential vector.



方案简介

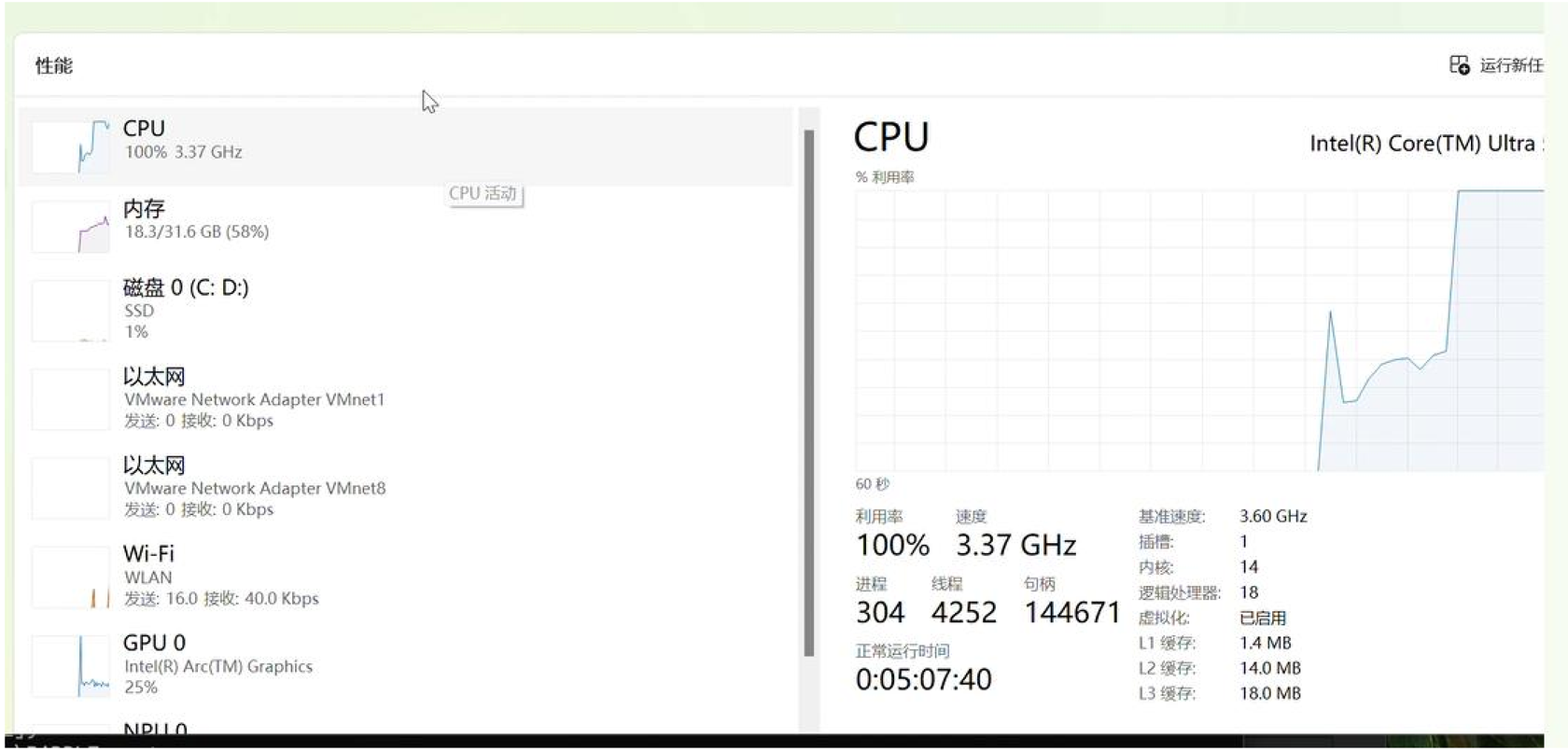
Program framework

The system combines the two-factor encryption mechanism of face and password, converts the face image to the hidden space through the encoder, and then inputs the face hidden vector and password into the transformer-based cryptography to get the encrypted hidden vector, and obtains the encrypted face image through the generator.

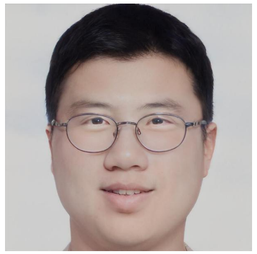
Encrypted face images are decrypted by the correct password when the user authenticates themselves and are used for face recognition.

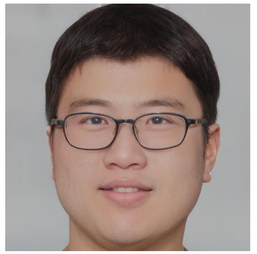
The designed system has efficient face privacy protection and identity recovery ability, realizing the balance of practicality and security.

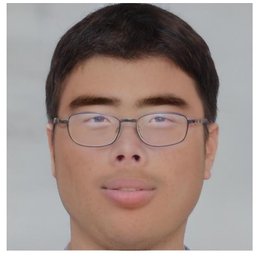
截屏说明

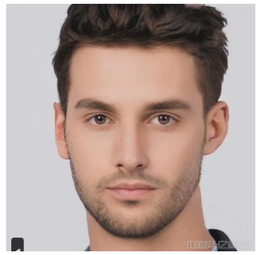


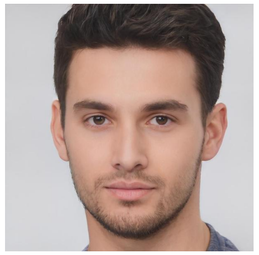
- BigDL Version 2.0: Used in a data analytics application running on Apache Spark. BigDL enables the processing and training of deep learning models directly within Spark's distributed computing environment, which is ideal for handling large-scale data efficiently.
- OpenVINO 2022.1: Integrated into a real-time video processing application to enhance performance. By optimizing deep learning models with OpenVINO, the application can run high-performance inference on Intel CPUs and GPUs, significantly improving the speed and efficiency of video analysis tasks.

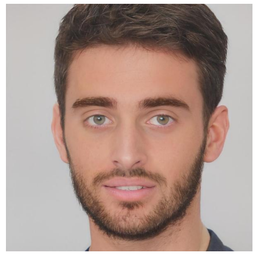


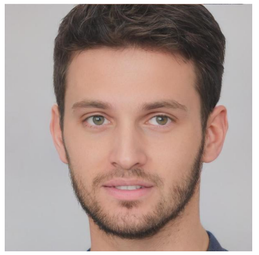












截屏说明

Original

Latent

Encrypted

Decrypted

Wrongly decrypted

方案总结

Advantages and characteristics

Points

Protect

We propose a face encryption recognition system based on generative model. The face image is encrypted and stored in the database, and it is decrypted for identification only at the time of authentication.

Two-factor

We propose a two-factor authentication that combines face and password. Only when the user provides the correct facial information and password can it be matched with the corresponding original facial image.

Generative model

This is the first attempt to use diffusion models for two-factor authentication systems, for protecting user privacy. It provides a more efficient, flexible and diversified privacy protection scheme.

隐私护卫团队