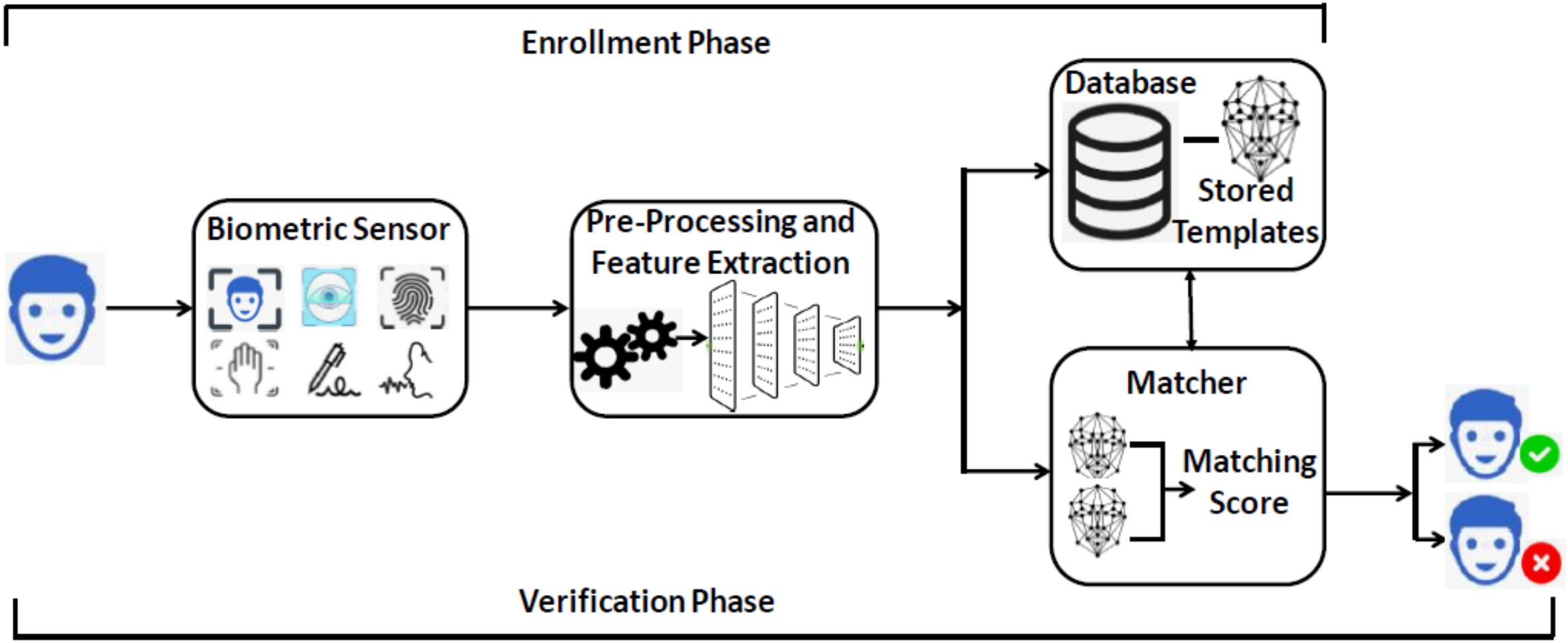
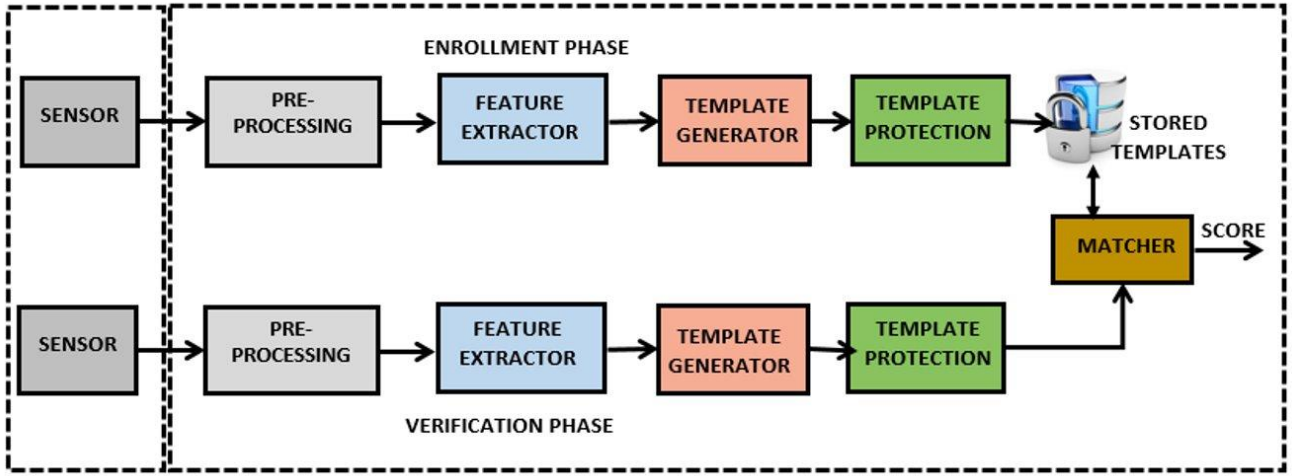
# Typical Biometric Recognition System

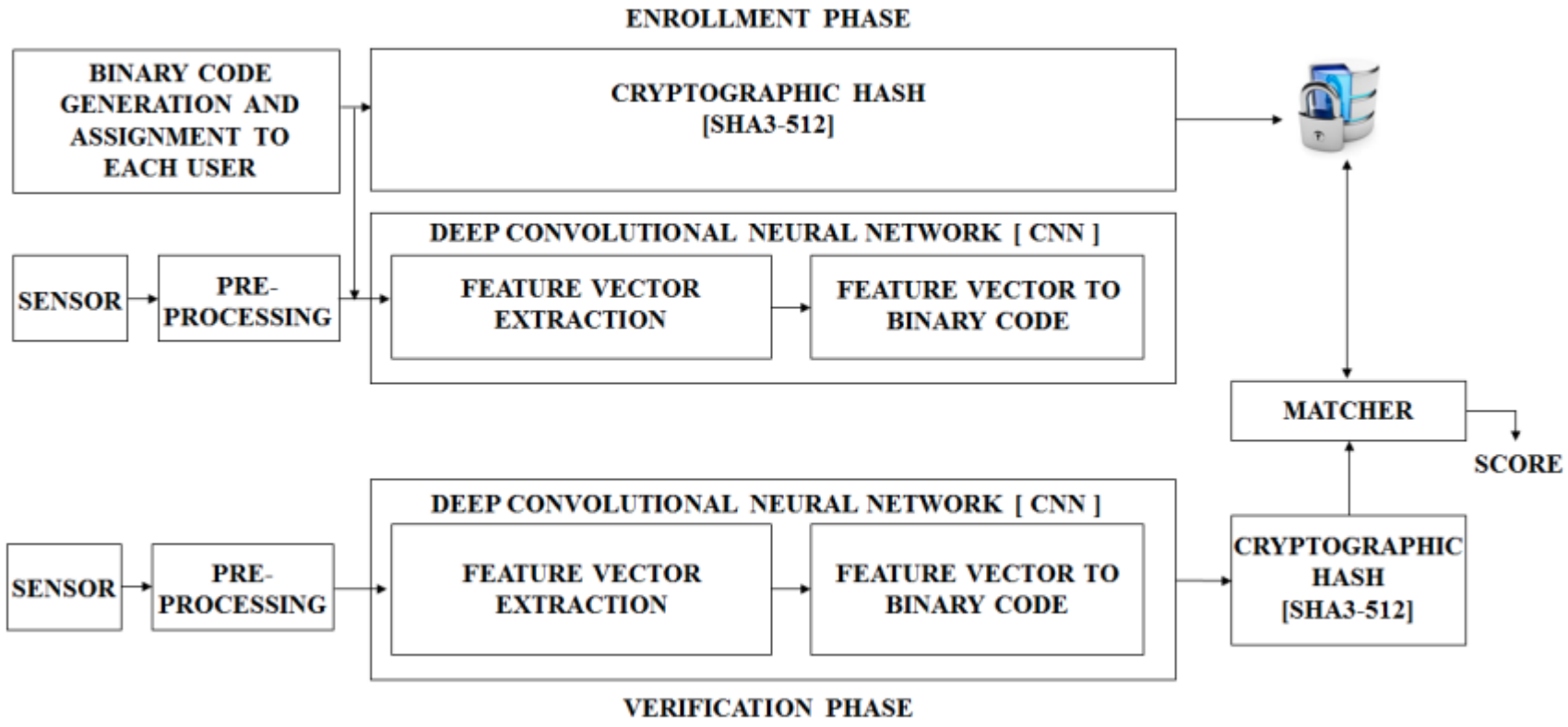


# Properties of an Ideal Biometric Template Protection Method

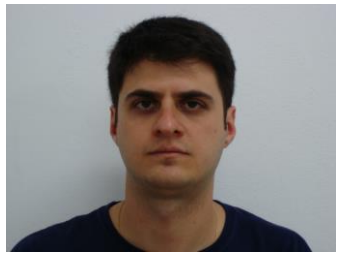



- **Security / Irreversibility** – It should be difficult to recover the unprotected template from the protected template.
- **Diversity / Unlinkability** – Two protected templates belonging to the same user should be far apart in space
- **Recognition Performance** – The recognition performance of the system should not drop beyond a reasonable limit after template protection is used.
- **Revocability** – It should be easily possible to revoke a protected template and generate a new template for the user.

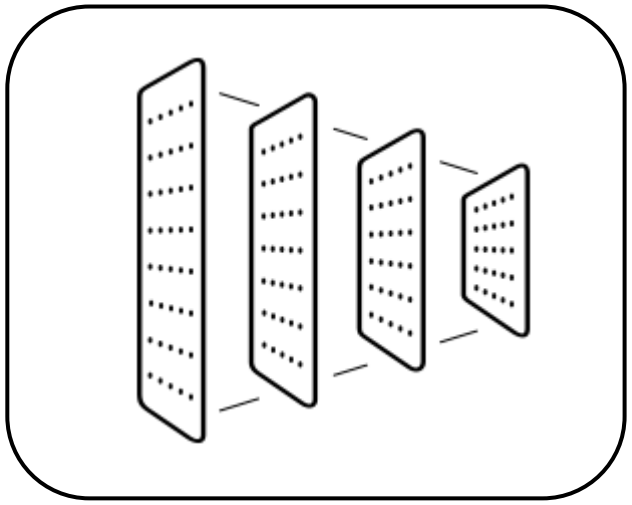
# Block Diagram of the Class of Biometric Template Protection Methods



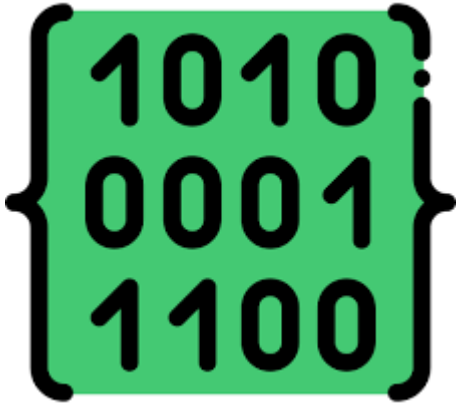
# Basic Block



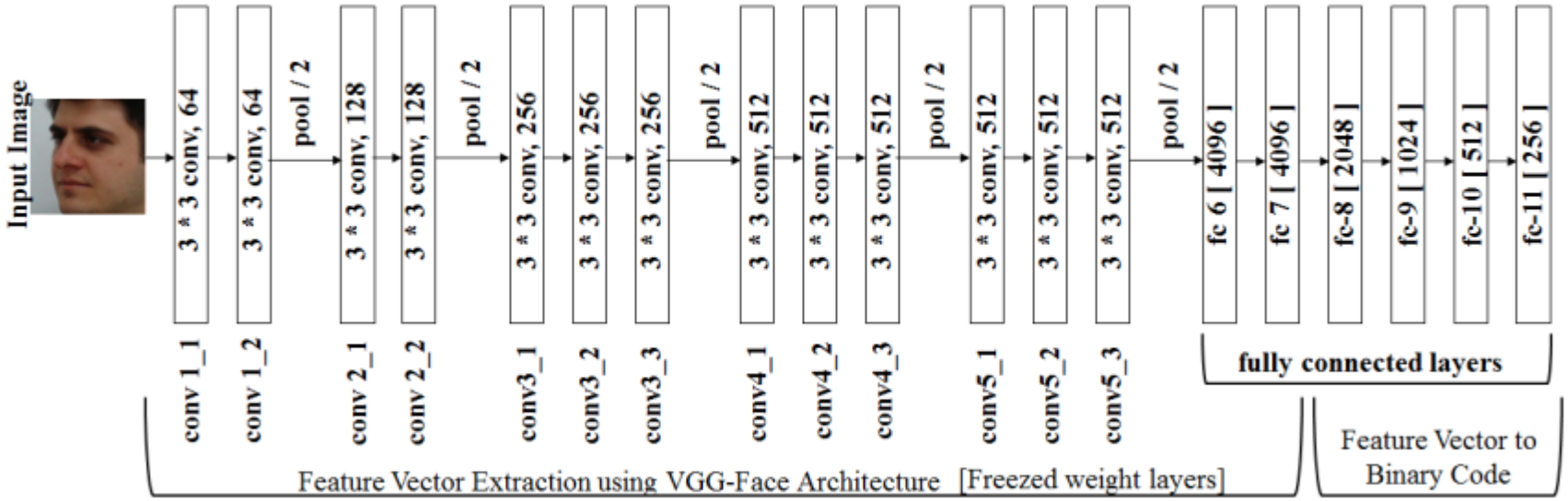
Face Image



Deep CNN Architecture




Maximum Entropy Binary (MEB) Code



# Face Recognition Models

- Different Face Recognition Models-
  - **Deep Face [Taigman et al, CVPR 2014]**
  - **DeepID [Sun et al, CVPR 2014]**
  - **FaceNet [Schroff et al, CVPR 2015]**
  - **VGG Face [Parkhi et al, BMVC, 2015]**
  - **SphereFace [Liu et al, CVPR 2017]**
  - **CosFace [Wang et al, CVPR 2018]**
  - **ArcFace [Deng et al, CVPR 2019]**
  - **Dlib**
  - **Center Triplet Loss [Zhao et al, IEEE Transactions on Multimedia 2020]**
  - **Universal Representation Learning [Shi et al, CVPR 2020]**
  - **Curricular Face [Huang et al, CVPR 2020]**
  - **MagFace [Meng et al, CVPR 2021]**
  - **Sface [Zhong et al, IEEE Transactions on Image Processing 2021]**
  - **Elastic Face [Boutros et al, CVPRW 2022]**
  - **AdaFace [Kim et al, CVPR 2022]**

Thank you