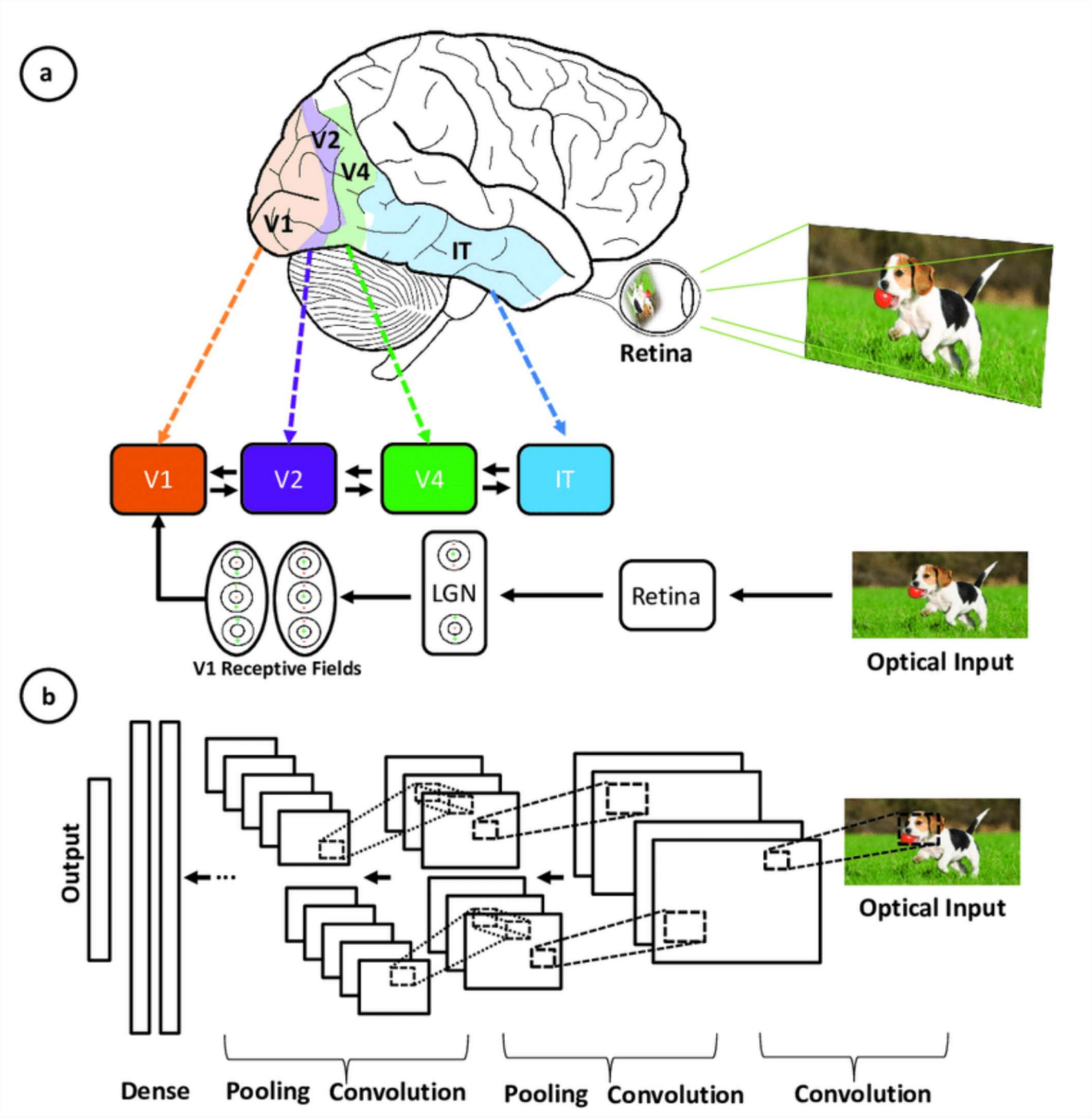
This article about using deep learning techniques to secure bioluminescent interfaces in the Internet of Bio Nano Things (IoBNT). The IoBNT is a network of nanoscale biological transceivers that collect information from the human body and communicate it to healthcare providers over the Internet. Bioluminescent bio-cyber interfaces (BBI) are used to connect these nanoscale devices, but they are vulnerable to external threat vectors due to their Internet connectivity.

The article discusses the use of deep learning algorithms to accurately classify anomalous BBI traffic patterns and improve security. The authors compare the performance of several deep learning models, including a hybrid convolutional and recurrent ensemble (CNN + LSTM), and find that it reported an accuracy of

approximately ~93.51% over other deep and shallow structures. The authors also highlight the benefits of using deep learning techniques for automatic feature extraction and selection, which eliminates the need for manual input feature selection.

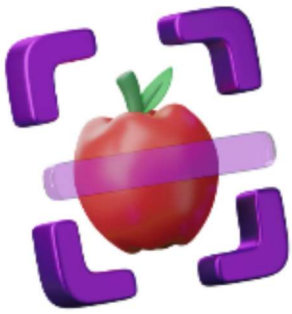
The article also discusses the potential deployment of the extracted optimal classifier in conventional intrusion detection systems as well as evolving non-Von Neumann architectures for real-time anomaly detection. The authors suggest that this approach could improve the security of IoBNT systems and help protect against bio-cyber terrorism.

Convolutional Neural Network

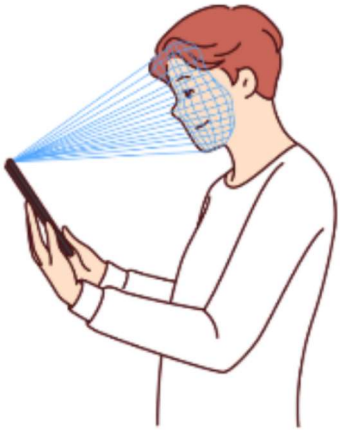


Some Practical Applications of CNN

Image classification



Object detection



Facial recognition

Zoumana K.

Long Short-Term Memory

0 - Close. 1 - Open.