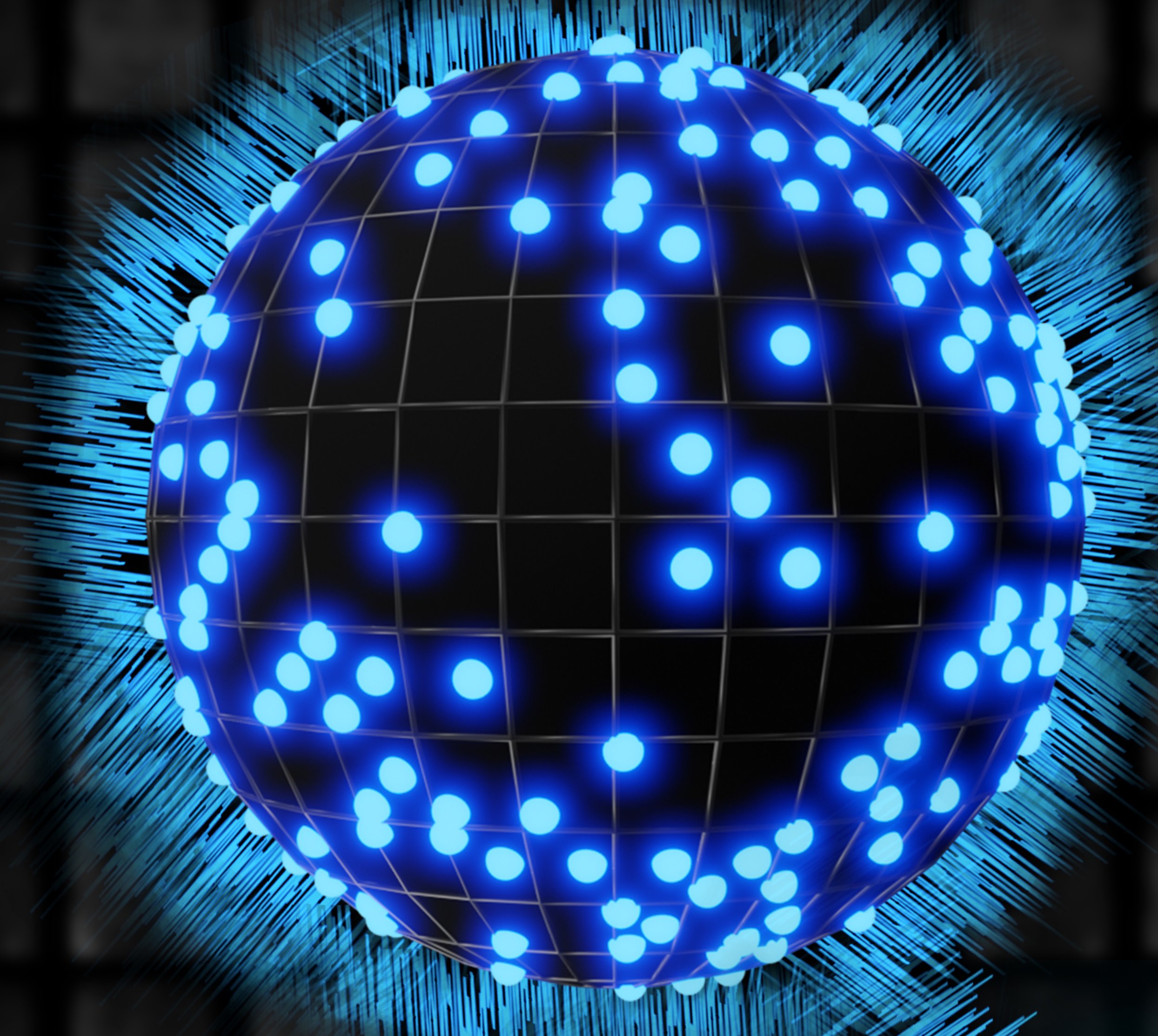

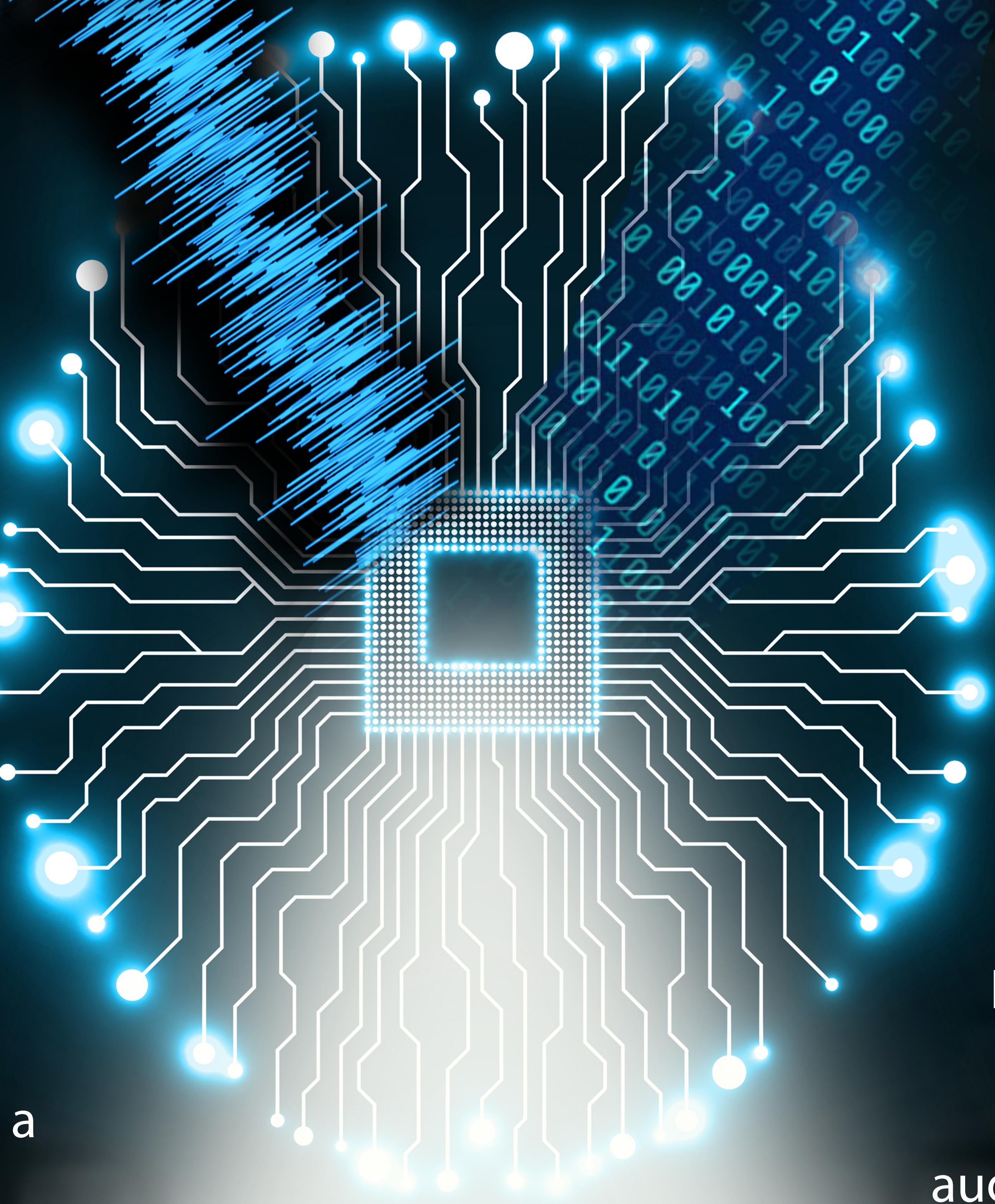

All over the world, people use biometrics as a means of authentication to secure access to confidential data. The convenience of presenting a biometric attribute instead of a traditional user verification technique, such as a long password, comes at a price. An imposter may try to imitate (spoof) the biometric attribute to gain illegal access. Presentation attack detection (PAD) systems can detect biometric spoofs presented to a sensor.

PAD systems are often the only gap between one's data and prying eyes. Although there are many antispoofing approaches, deep-learning-based approaches have shown promising results. However, one of the limitations of deep learning is the lack of data to train a robust model. We combat this limitation using generative adversarial networks to produce more images to augment the original dataset.

Improving Face Presentation Attack Detection using Deep Learning and Generative Data Augmentation

Jarred Orfao & Prof. D.T. van der Haar

UNIVERSITY OF JOHANNESBURG

binary: https://www.scienceabc.com/wp-content/uploads/ext-www.scienceabc.com/wp-content/uploads/2019/08/Abstract-Technology-Binary-code-Background.Digital-binary-data-and-Secure-Data-Concept-VectorFotomays.jpg-.jpg
noise: noise signal: https://miro.medium.com/max/960/1*sBmLLMR5XLgPwST6vRqKaQ.png
brain: https://i1.wp.com/bdtechtalks.com/wp-content/uploads/2019/06/artifiical-intelligence-circuit-brain.jpg?fit=4155%2C4155&ssl=1

CASIA: Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi and S. Z. Li, "A face antispoofing database with diverse attacks," 2012 5th IAPR International Conference on Biometrics (ICB), 2012, pp. 26-31, doi: 10.1109/ICB.2012.6199754.