Acta Scientific COMPUTER SCIENCES

Volume 6 Issue 6 June 2024

Editorial

Infallible Biometric Verification

Lavanya Srinivasan*

School of Computing and Engineering, University of West London, United Kingdom

***Corresponding Author:** Lavanya Srinivasan, School of Computing and Engineering, University of West London, United Kingdom.

Received: May 21, 2024

Published: May 30, 2024

Biometrics is to identify individuals based on their distinctive traits. Fingerprinting has been a conventional method. Iris scanning, facial recognition, and gait are examples of modern techniques. All current methods share the same flaw, nothing stops a malevolent impostor who wants to pose as someone else and replicate that person's biometric traits known as deepfake. Cybersecurity is significantly challenged by deepfake technology. One fundamental flaw in all current approaches is that none of the laws of physics can guarantee or quantify their security.

Quantum biometrics, whose working principles rely on the quantum mechanics of photodetection and the capacity of the human visual system to execute photon counting, provide unbreakable security. The loss of optical information as light travels from the eyeball to the retina is illustrated in Figure 1. The losses can be calculated using the known photon number of a brief light pulse that strikes the eye and the test subject's reaction statistics regarding whether they see the light flash.

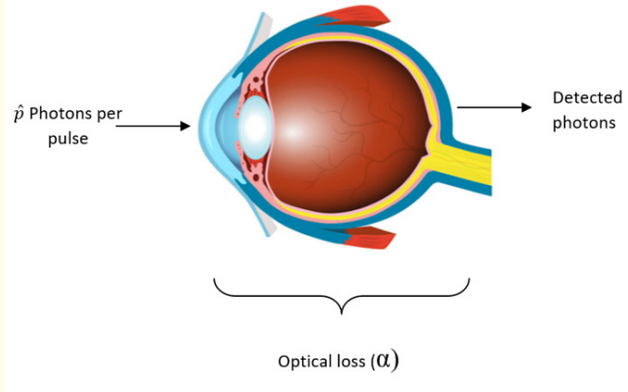

Figure 1: Human visual system.

An intricate "quantum fingerprint" that involves the retina, brain, and eye is examined using a special kind of light that stimulates the visual system of the fingerprint. Quantifying the optical losses involves using a parameter α, or more accurately, an entire α-map obtained from many optical routes connecting the cornea and the retina. The approach yields remarkable performance, with a false-positive identification probability of less than 10^(-10). To break the security a pretender must have access to quantum technology, which is not anticipated to be available for many decades. Specifically, this includes quantum thermometry and magnetometry with an energy resolution of at least 10^(-9).

An identification technique is based on simultaneously illuminating multiple low-α pixels and selecting and illuminating large-α pixels on the retina which produce a pattern that the user can recognize. In low-α pixels, even with an ideal photodetector, the impostor will view all pixels as illuminated, but the user will not sense any light. Individual subjects exhibit varying optical losses along the beam path from the eyeball to the retina.

The demand for safe identifying systems is constantly increasing, making security a serious concern on a global scale in recent times. In the future, Hyper-realistic deepfakes can be overcome by quantum fingerprint.