Abstract

Current biometric security methods, while widespread, have prominent deficiencies. Biometric authentication combats issues created by insecure passwords; a good password can properly protect devices and accounts from attacks, but most people do not set secure passwords, and studies show that almost 60% of users create passwords including names or birthdays (ASEE 2022). Biometric authentication is used by many devices – including cell phones, keypads, computers, and locks – but many of these systems are not very secure. These insecurities compromise personal informational security, making it more difficult to prevent malicious users from accessing the device. This project aims to address these insecurities by writing a program to reinforce biometric authentication systems using two novel technologies: hyperdimensional vectors and fuzzy signatures. This model first takes in a facial input, identifies the face, and extracts facial features. These features are combined into a numerical string used to generate the hypervectors, which are then compared. This program can be used to improve the security of biometric authentication systems everywhere. In the future, it will be relevant to improve the program in terms of efficiency, security, and more. The system has flaws such as struggles with facial identification in non-ideal lighting and angles, and these can be repaired later.

Keywords: biometric authentication, facial ID, hypervectors, hyperdimensional, fuzzy extractor