Deep Learning-based Biometric Homomorphic Encryption

ABHISHEK SR - MCA23-103

Abstract

In contemporary digital security systems, the generation and management of cryptographic keys, such as passwords and pin codes, typically rely on stochastic random processes and intricate mathematical transformations. While these keys offer robust security, their storage and distribution demand sophisticated and costly mechanisms. This study explores an alternative approach that leverages biometric data for generating cryptographic keys, thus eliminating the need for complex storage and distribution processes. The paper investigates biometric key generation technologies using deep learning models, specifically employing convolutional neural networks (CNNs) to extract biometric features from human facial images. Subsequently, code-based cryptographic extractors process the primary extracted features. The performance of various deep learning models and the extractor is evaluated by considering Type 1 and Type 2 errors. Optimized algorithm parameters yield an error rate of less than 10%, making the generated keys suitable for biometric authentication. Additionally, this study demonstrates that the application of code based cryptographic extractors provides a post-quantum level of security, further enhancing the practicality and effectiveness of biometric key generation technologies in modern information security systems. This research contributes to the ongoing efforts towards secure, efficient, and user-friendly authentication and encryption methods by harnessing the power of biometric data and deep learning techniques.

Reference

1. Kuznetsov, O., Zakharov, D., & Frontoni, E. (2023). Deep learning-based biometric cryptographic key generation with post-quantum security. Multimedia Tools and Applications, 83(19), 56909–56938. https://doi.org/10.1007/s11042-023-17714-7

2. Singh, M., Baranwal, N., Singh, K., Singh, A., & Zhou, H. (2023). Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression. Journal of Information Security and Applications, 79, 103628. https://doi.org/10.1016/j.jisa.2023.103628

3. Yang, W., Wang, S., Hu, J., Tao, X., & Li, Y. (2024). Feature extraction and learning approaches for cancellable biometrics: A survey. CAAI Transactions on Intelligence Technology. https://doi.org/10.1049/cit2.12283