Deep Secure Quantization: On Secure Biometric Hashing against Similarity-Based Attacks

Yanzhi Chen, Yan Wo, Renjie Xie, Chudan Wu, Guoqiang Han

PII: S0165-1684(18)30297-4
DOI: https://doi.org/10.1016/j.sigpro.2018.09.013
Reference: SIGPRO 6923

To appear in: *Signal Processing*

Received date: 1 February 2018
Revised date: 7 August 2018
Accepted date: 10 September 2018

Please cite this article as: Yanzhi Chen, Yan Wo, Renjie Xie, Chudan Wu, Guoqiang Han, Deep Secure Quantization: On Secure Biometric Hashing against Similarity-Based Attacks, *Signal Processing* (2018), doi: https://doi.org/10.1016/j.sigpro.2018.09.013

Highlights

- This paper proposes a novel deep neural network-based biometric hashing framework;
- It offers strong resistance to both conventional ciphertext-only attacks and recent similarity-based attacks;
- We analyze why existing biometric hashing models are vulnerable to similarity-based attack;
- Our work suggests new definition of non-invertibility in biometric hashing.