Hui **Zhang**

(+86) 19810919882 | huizhang@stu.ahu.edu.cn | 01cv

Research statement

Face reconstruction attack and protection: This is a topic I am currently working on in my PhD. The ubiquitous use of face recognition has sparked increasing privacy concerns, as unauthorized access to sensitive face images could compromise the information of in dividuals. Researches have shown that once deep face feature are derived from original facial images, they can be reverse-engineered by reconstruction attack model, potentially revealing sensitive user details like gender and ethnicity, or masquerading as legitimate users to obtain service authorization. Therefore, our goal is to construct an efficient reconstruction attack model and give countermeasures in a black-box scenario.

Keywords: Face recognition; Templete Invertion Attack; Biometric Templete Protection.

Biometric authentication protocol: With the rapid development of Internet technology and hardware equipment, biometric recognition has been widely used in many fields. Compared with the traditional password-based authentication, biometric authentication has the advantages of uniqueness, persistence and convenience, which solves the problems of password authentication scheme, such as dependence on user memory and complicated password design. However, the rapid proliferation of biometric-based authentication systems for identity management calls urgent attention due to the fact that biometrics and users are permanently connected and coupled, which usually contains a lot of sensitive information of users. There, our goal is to design a secure biometric authentication and key agreement protocol for complex network environments.

Keywords: Identity Authentication; Multi-server Authentication; Mutual Authentication.

Federated Learning based fetal anatomical structure detection: To our knowledge, fetal anatomical structure detection is an essential basis for diagnosing diseases, and some diseases can be diagnosed directly in the presence of key anatomical structures. For example, the absence of cavum septi pellucidi structure in fetal head view is diagnosed as a severe disease called holoprosencephaly. Recently, deep learning (DL)-based methods as a powerful tool have already achieved much progress in fetal anatomical structure detection, such as fetal standard view quality control, and disease-assisted diagnosis. However, DL-based models often rely on a large quantity of high-quality annotated data to achieve optimal performance. Given that fetal ultrasound data is distributed across different medical institutions and due to concerns regarding data security and privacy, there exist data silos between these institutions, preventing secure data sharing. Furthermore, models trained independently by different institutions cannot achieve global optimization.

Keywords: Medical Image; Federated Learning; Domain Adaptation.

Publications

Journal

- **Hui Zhang**, Xuejun Li, Syh-Yuan Tan, Ming Jie Lee, Zhe Jin. "Privacy-Preserving Biometric Authentication: Cryptananlysis and Countermeasures." ***IEEE Transactions on Dependable and Secure Computing*** (2023).
- **Hui Zhang**, Weixin Bian, Biao Jie, Deqin Xu and Jun Zhao. "A Complete User Authentication and Key Agreement Scheme Using Cancelable Biometrics and PUF in Multi-Server Environment." ***IEEE Transactions on Information Forensics and Security*** (2021).
- **Hui Zhang**, Weixin Bian, Biao Jie and Shuwan Sun. "BioP-TAP: An efficient method of template protection and two-factor authentication protocol combining biometric and PUF." ***Journal of Intelligent & Fuzzy Systems*** (2022).
- Jun Zhao, Weixin Bian, Deqin Xu, Biao Jie and **Hui Zhang**. "A Secure Biometrics and PUFs-Based Authentication Scheme With Key Agreement For Multi-Server Environments." ***IEEE Access*** (2022).

Conference

- **Hui Zhang**, Xingbo Dong, YenLung Lai, Ying Zhou, Xiaoyan Zhang, Xingguo Lv, Zhe Jin and Xuejun Li. "Validating Privacy-Preserving Face Recognition under a Minimum Assumption ." ***The IEEE/CVF Conference on Computer Vision and Pattern Recognition 2024.*** (CVPR2024).
- **Hui Zhang**, Jiewen Yang, Xingbo Dong, Xingguo Lv, Zhe Jin and Xuejun Li. "A Video Face Recognition Leveraging Temporal Information based on Vision Transformer ." ***The 6th Chinese Conference on Pattern Recognition and Computer Vision*** (PRCV2023).
- **Hui Zhang**, Weixin Bian, Biao Jie and Shuwan Sun. "A Novel Method of Template Protection and Two Factor Authentication Protocol Based on Biometric and PUF." ***The 13th International Symposium on Cyberspace Safety and Security*** (CSS2021 oral).
- Dezhi Li, Hojin Park, Xingbo Dong, Yenlung Lai, **Hui Zhang**, Andrew Beng Jin Teoh and Zhe Jin."Minimum Assumption Reconstruction Attacks: Rise of Security and Privacy Threats against Face Recognition." ***The 6th Chinese Conference on Pattern Recognition and Computer Vision*** (PRCV2023).
- Xingguo Lv, Xingbo Dong, Zhe Jin, **Hui Zhang**, Siyi Song and Xuejun Li ."L2DM: A Diffusion Model for Low-Light Image Enhancement." ***The 6th Chinese Conference on Pattern Recognition and Computer Vision*** (PRCV2023).
- Ying Zhou, Ming Jie Lee, **Hui Zhang**, Xingbo Dong and Zhe Jin."Random Undersampling and Local-global Matching Mechanism for Cancellable Biometrics Against Authentication Attack." ***The 17th Chinese Conference on Biometric Recognition*** (CCBR2023 oral).
- Yafei Liu, Ying Zhou, Weiyu Zhou,**Hui Zhang**, Yufang Dong, Xingbo Dong and Zhe Jin."SP2IN: Leveraging Fuzzy Commitment and LDPC Sum-Product Decoder for Key Generation from Face." ***The 17th Chinese Conference on Biometric Recognition*** (CCBR2023 oral).

Education

College of Computer Science and Technology, Anhui University *Hefei, P.R.China*

PH.D, COMPUTER SCIENCE AND TECHNOLOGY *Sep. 2022 - now*

- Thesis: Privacy-preserving face recognition scheme against reconstruction attack. Supervisor: Prof. Jin Zhe, Prof. Li Xuejun.

College of Computer and Information, Anhui Normal University *Wuhu, P.R.China*

MSC.,COMPUTER SCIENCE AND TECHNOLOGY *Sep. 2019 - Jun. 2022*

- Thesis: Study on User Identity Authentication Scheme Based on PUF and Cancelable Biometrics. Supervisor: Prof. Bian Weixin.

College of Computer Science and Technology, Huaibei Normal University *Huaibei, P.R.China*

BSC., DIGITAL MEDIA TECHNOLOGY *Sep. 2015 - Jun. 2019*

- Thesis: Vehicle license plate recognition system based on MATLAB. Supervisor: Dr. Guo Guifang.

Competitions

1 The 10th China College Student Computer Design Competition. **(National Silver Award, Provincial Gold Award)**
2 The 6th "Internet +" College Students Innovation and Entrepreneurship Competition **(Provincial Silver Award)**
3 CCF China Service Computing Competition **(Bronze Award)**
4 2020 Wuhu Wealth Creation Competition **(The Most Popular Award)**

Awards

1 National Scholarship for Doctoral Students 2022-2023
2 Excellent master thesis of Anhui Computer Society
3 Model Student of Academic Records 2020-2021
4 Excellent Student Cadre 2019-2020

Skills

Certificates Database System Engineer, Software Design Engineer
Programming Python, Matlab, C, C++
Databases MySQL, Oracle
Languages I speak Mandarin and English

Professional Services

Invited to Review: IEEE Transactions on Information Forensics and Security, IEEE Transactions on Biometrics, Behavior, and Identity Science, IEEE Access, IEEE International Joint Conference on Biometrics (IJCB 2023) ACM International Conference on Multimedia (ACMMM 2023), International Conference on Computer Vision (ICCV 2023).