Automatic Feature Detection/Recognition for Improved User Identity Management and Data Protection

Category: Technology Maturity Assessment

Most Relevant Research Agenda Topics:

https://thearea.org/area-research-agenda/biometric-identification-of-wearable-enterprise-ar-device-users/

https://thearea.org/area-research-agenda/automatic-detection-and-obfuscation-of-facial-and-or-personal-data-of-people-in-ar-user-vicinity/

Data protection and privacy How will AR when used with Remote video functionality protect peoples faces and company IP (information visible in background, people waling past)	3.8 ★★★★☆	(11 👤)
Integration of devices into the corporate network (Identity management, application of corporate cyber security rules) The effectiveness of RA is subject to access to company data that can often be confidential.	3.6 ★★★⯪☆	(9 👤)
In order to reduce the need for text input when starting a session, we need Biometric Identification of Wearable Enterprise AR Device Users Biometric identification will increase reliability of authentication & reduce the need for users to use text input, increasing risk manager confidence	3.3 ★★★☆☆	(10 👤)

Current Situation

- There is insufficient use of automation/automatic detection and recognition of features of users in AR system authentication
  - Users must be trained in and follow “manual” AR system authentication steps
  - Authentication systems may be developed (internally) and connected to internal databases (employee, work order, project management, etc) without biometric tools
  - Systems that are time consuming and/or prone to error are removed/disabled
- Low/lack of automatic detection/recognition of environmental features increases risk of relying entirely on users’ behavior to avoid exposure of or inappropriate use of sensitive information in the AR system camera’s view (e.g., faces and company-confidential intellectual property)

Problems this Research Would Address

- Users of shared devices or users who do not frequently use AR systems must manually identify themselves to authenticate and get access to AR experiences
  - Identification and authentication processes are **slow, error prone and may put users off**
- Low documentation (and understanding) of the potential pros and cons and low use of high-performance automated detection and identification of features for user authentication among AR designers/developers, systems integrators, internal IT departments and end users leads to **low/poor use of the latest innovation in the biometric field** for purpose of automatic AR system user authentication
- Due to users avoiding or being unaware of procedures, AR providers and customers with AR in the field are exposed to risks associated with unintentional **exposure of information (IP)** and **identities of people in the AR system user's environment**
  - Risk managers and IT departments do not approve use of AR systems in some (e.g., remote assistance) or all use cases which could lead to exposure

Possible Questions the Research Would Answer

- How can integrating automated feature detection/recognition systems increase use and reduce risk of AR systems in the workplace?
- What is the state of the art in commercially-available tools for industrial-grade biometric authentication systems/solutions/services and other automatic feature recognition libraries?
- Are there tools that can detect/use unique human features to securely and reliably identify and authenticate users for access to devices and specific AR experiences?
- Are there technologies commercially available for automatic visual and/or auditory feature detection and obfuscation that could be used by AR providers and customers to reduce or eliminate risks associated with **exposure of information (IP)** and **identities of people** in the AR user environment?

Whose problem would be addressed?

- *IT groups and enterprise AR project managers* would be better prepared
  - To assess suitability and identify viable options for integrating automatic feature detection, such as biometric identification, as the basis for AR user identification and authentication
  - To discuss with suppliers and internal stakeholders how use of automatic detection and obfuscation of IP and/or nearby users could improve operation and reduce risks
- *Providers of enterprise wearable AR displays and enterprise AR software/platform companies* would be able
  - To identify potential providers/partners to supply new enabling technologies to increase differentiation in the ecosystem and offer unique value to their customers
  - To develop new value-added components, systems or services for enterprise AR use to generate higher revenues and RoI

How would this research be conducted?

1. The research partner chosen for this project will have extensive background in development of automatic feature (e.g., biometric) technologies and deep connections with leaders in the automatic feature detection/id ecosystem
2. Desk research would generate documentation about the current options, leading suppliers and sources of secondary information
3. In a laboratory environment using one enterprise IT system for identification and authentication with two types of AR systems, a testing method will be developed and two or more biometric identification tools evaluated
4. The testing in a lab setting would also permit comparison of interfaces and robustness with at least four different users and/or other variables TBD
5. A report, including a gap analysis, description of testing methodology developed, results of testing and set of recommendations for future work will be prepared

Deliverables of this project

- An annotated table (in a spreadsheet) of automatic feature detection and identification (and obfuscation) technologies, providers and description of systems in use in enterprise today
- A tool for AREA members to assess/estimate potential benefits of automatic feature detection, identification and obfuscation technologies in different use cases and environments
- Report describing the potential opportunity for use of automatic feature detection to increase use and reduce risk, including a gap analysis, description of testing methodology developed, results of testing and set of recommendations for future work
- Executive summary of findings for public release and a webinar

Benefits to AREA members

- Insights into how integration of automatic feature detection technologies with AR system authentication and use in workplace environments could increase use by employees that need to be authenticated and decrease risk by reducing reliance on modification of user behavior
- Assessment of the maturity of technologies for potential integration
- If/when automatic feature detection technologies can be used for AR system access and to reduce risk, this project will be the basis for evaluating potential providers, and for testing suitability of available options