Security and Privacy concerns on Artificial Intelligence-based Emotion Recognition Systems

Lala Shahbandayeva
ADA University
Baku, Azerbaijan
lshahbandayeva2019@ada.edu.az

Abstract

Emotions play a crucial role in people's daily lives. They are in every part of their day and convey information in a clear way during the communication. Apart from the communication among humans, it is crucial to convey emotions while interacting with devices. This brings an important ingredient to the traditional Human-Computer Interaction which is to enhance the concept with emotion detection. The ability to understand how the emotions are conveyed among people through devices/software becomes important when designing new technologies for people.

Emotion recognition can be used by companies to provide personalized information such as advertisements [1]. As a case in point, it can show the how mental health affect people's life on social media platforms like Facebook, Instagram etc. [1][2][3]. Moreover, emotion recognition systems can be used to share the information to the people who most probably will reflect to those thorough behavioral implications [1][4][5]. However, the usage of some data such as age, location, messages, etc. while providing personalized content can cause privacy issues [6][7][8]. Therefore, some researchers conducted studies to provide information about the security, privacy and ethical effects of usage of such technologies [9][10].

Although in traditional HCI, emotions did not play a significant role whether it is chatbots or digital voice assistants such as Alexa, Siri etc. in the past, currently Artificial Intelligence (AI) based emotion detection is becoming increasingly popular in everyday activities. AI-based emotion recognition systems can read people's feelings through text, voice tone, facial expressions, and gestures and can change their behaviors based on that which introduces three main problems. The first problem is the bias which happens in the most AI applications with the use of bias datasets. The second problem is privacy which covers keeping people's personal data private. The third problem is the use of mass surveillance which is about the possibility of detecting people's emotions through surveillance cameras and use by the government.

To solve these potential problems, it is crucial to further analyze the importance and privacy concerns of emotion detection and recognition in Human-Computer Interaction/Human-AI Interaction. The research was conducted by surveying 72 participants aged between 15 and 58. The survey includes the opinions of participants about the security and privacy concerns of AI-based emotion detection systems. The result of the conducted surveys and interviews shows that in general, people are not pessimistic about the AI-based emotion detection systems.

This research introduces the emotion recognition in Human-Computer Interaction and describes the general understanding, importance and privacy concerns in emotional Human-Computer Interaction/Human-AI Interaction. The findings explain that though some people believe that AI-based emotion recognition systems can cause security and privacy issues, the higher percentage of people are optimistic about the good usage of these technologies.

CSS Concepts: Human-centered computing → Empirical studies in HCI

Keywords: Emotion recognition, chatbots, digital voice assistants, privacy.

Bibliography

[1] Andrew McStay. 2018. Emotional AI: The Rise of Empathic Media. SAGE.

[2] Louise Matsakis. 2018. Online Ad Targeting Does Work—As Long As It's Not Creepy. Wired

[3] Ysabel Gerrard and Tarleton Gillespie. 2019. When Algorithms Think You Want to Die. Wired.

[4] Anthony Nadler and Lee McGuigan. 2018. An impulse to exploit: the behavioral turn in data-driven marketing. Critical Studies in Media Communication.

[5] Shoshana Zuboff. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Social Science Research Network, Rochester, NY.

[6] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012).

[7] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI 2014), 2347–2356. https://doi.org/10.1145/2556288.2557421

[8] Igor Bilogrevic, Kévin Huguenin, Berker Agir, Murtuza Jadliwala, Maria Gazaki, and Jean-Pierre Hubaux. 2016. A machine-learning based approach to privacy-aware information-sharing in mobile social networks. Pervasive and Mobile Computing 25: 125– 142.

[9] Eric P.S. Baumer, Timothy Berrill, Sarah C. Botwinick, Jonathan L. Gonzales, Kevin Ho, Allison Kundrik, Luke Kwon, Tim LaRowe, Chanh P. Nguyen, Fredy Ramirez, Peter Schaedler, William Ulrich, Amber Wallace, Yuchen Wan, and Benjamin Weinfeld. 2018. What Would You Do?: Design Fiction and Ethics. In Proceedings of the 2018 ACM Conference on Supporting Groupwork (GROUP 2018), 244–256.

[10] Lydia Manikonda and Munmun De Choudhury. 2017. Modeling and Understanding Visual Attributes of Mental Health Disclosures in Social Media. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI 2017), 170–181.