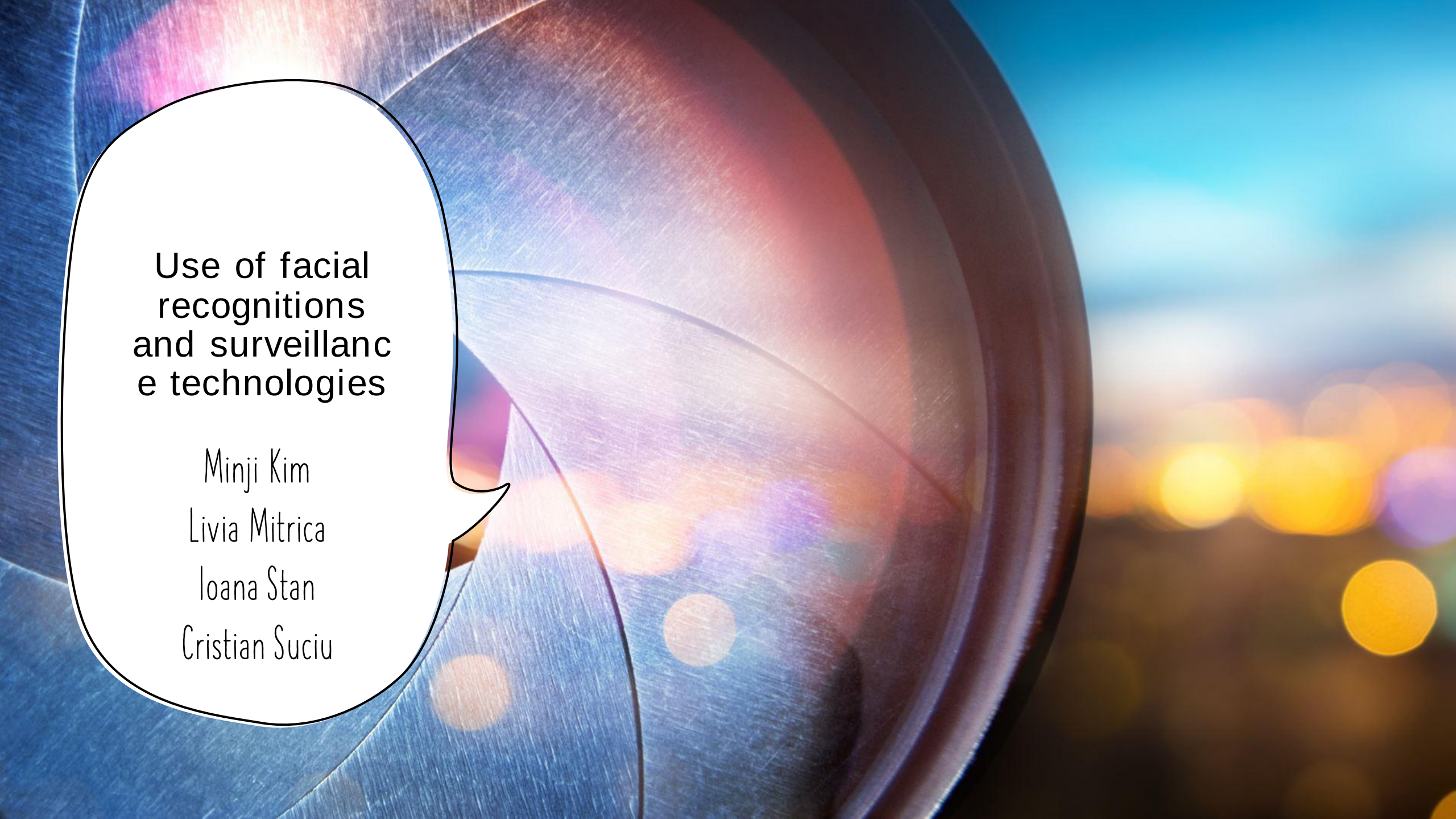
Use of facial recognitions and surveillanc e technologies
Minji Kim
Livia Mitrica
Ioana Stan
Cristian Suciu

FORGERY AND MANIPULATION

- Criminals may attempt to manipulate facial recognition systems using techniques such as deepfakes or other forms of facial manipulation to deceive the technology.
- An example of a deep fake video that manipulates people into thinking that president Zelensky is surrendering to Russia

SOCIAL PROFILING AND DISCRIMINATION

- Facial recognition systems may unintentionally perpetuate and exacerbate societal biases. If these systems are trained on biased data, they can lead to discriminatory outcomes, targeting certain demographics unfairly.

ROUND 2, ARGUMENTS

- Facial recognition proves to be an unreliable tool for Search & Rescue missions, as it has the potential to inadvertently perpetuate and worsen societal biases. Consequently, relying solely on this technology may lead to inaccurate or biased outcomes, hindering the effectiveness of rescue efforts.

First Scenario - Search and Rescue

- Facial recognition can be used in search and rescue operations. Surveillance technologies can assist in quickly locating missing persons or individuals in emergency situations.
- For example: Imagine a situation where a child goes missing in a crowded public area, such as a shopping mall or amusement park. In this scenario, facial recognition technology can be employed to accelerate the search process. Also, with facial recognition and different surveillance cameras, the track of movements can be reproduced.

ROUND 2, ARGUMENTS

- While implementing facial recognition in larger scale operations, like boarding an airplane, holds promise for security enhancement, it's crucial to address a vulnerability. The rise of deepfake technology poses a significant threat, allowing malicious actors to exploit and trick facial recognition systems.
- For example, one could use a 3D printed mask from a deep fake model.

Second Scenario - Access Control and Authentication

- Facial recognition can be used for secure access control in various settings, such as airports or corporate offices. This technology provides an efficient means of verifying identity, reducing the reliance on traditional access methods like ID cards or passwords.
- For example: London airport allows passengers to use self-service boarding gates equipped with facial recognition technology. As travelers approach the gate, cameras capture facial images and compare them to the stored biometric data associated with the individual's passport or travel documents.

THANK YOU!

Use of facial recognitions and surveillance technologies

Fair team

Chereji Iulia

Cotor Catinca

Iacob Victor

First Scenario - Search and Rescue

- Facial recognition can be used in search and rescue operations. Surveillance technologies can assist in quickly locating missing persons or individuals in emergency situations.

- For example: Imagine a situation where a child goes missing in a crowded public area, such as a shopping mall or amusement park. In this scenario, facial recognition technology can be employed to accelerate the search process. Also, with facial recognition and different surveillance cameras, the track of movements can be reproduced.

Second Scenario - Access Control and Authentication

- Facial recognition can be used for secure access control in various settings, such as airports or corporate offices. This technology provides an efficient means of verifying identity, reducing the reliance on traditional access methods like ID cards or passwords.
- For example: London airport allows passengers to use self-service boarding gates equipped with facial recognition technology. As travelers approach the gate, cameras capture facial images and compare them to the stored biometric data associated with the individual's passport or travel documents.

Round 2

- Solution for Forgery and Manipulation: Combine facial recognition with other biometric modalities, such as fingerprint or iris recognition. Multi-modal biometrics enhance security by requiring attackers to replicate multiple biometric traits, which is significantly more difficult.
- Solution for social profiling and discrimination: Developers should actively work to identify and rectify biases in the training data and algorithmic models. They should also use more diverse and representative datasets during the training phase to ensure that the algorithms are trained on a wider range.

Sources

- ChatGPT