Should facial recognition systems be regulated?

David Garcia Arias

Facial recognition systems

A facial recognition system is a technology used to identify or verify a person’s identity from digital images or videos. It generally works by matching facial features from images stored in a database.

Facial recognition systems

Facial recognition systems have lower accuracy than fingerprint and iris recognition systems. They tend to be affected by the level of light, angle of the picture or video, and facial expression. However, they are contactless and can be applied from a bigger distance than fingerprint and iris recognition systems, and without the person’s permission.

They are used for human-computer interaction, video surveillance, as a commercial identification and marketing tool, etc.

Facial recognition systems

Facial recognition is carried out in two steps:

- First, the system extracts features from a face’s image and selects them.
- Second, it classifies the group of features extracted, looking for a match.

Techniques for face acquisition

- Traditional.
- 3D recognition: it is less affected by the level of light and the angle the pictures are taken from than the traditional approach.
- Skin texture analysis: adding skin texture analysis to another method can improve its efficacy between 20 and 25%.
- Thermal cameras.
- A combination of some of the above methods.

Applications

- Social media:
  - New functionalities in social media.
  - ID verification.
- Security services:
  - Airports.
  - Public events.
  - Streets of London from 2016 to 2019.
  - Different cities in the USA, China, Netherlands, and South Africa.

Challenges and ambiguities

- Affected by the level of light, angle of the picture or video and facial expression.
- It has the highest false acceptance and rejection rates among biometric systems.
- Ineffective when working with large databases. It gives several possible matches and a human needs to decide if any of them is right. This leads to targeting the wrong person sometimes.
- Lower false non-match rate for black people, women and very white people.

Possible solutions

- In order to minimize these drawbacks the following measures can be implemented:
  - Better lighting.
  - 3D recognition.
  - Larger databases with thousands of pictures of every individual from different angles and with different facial expressions.
  - Combine traditional or 3D techniques with skin texture analysis or thermal cameras.

Data privacy ambiguities

- The objects stored in a database can be hacked and lead to identity fraud.
- Privacy is compromised by surveillance technologies. It is thought by some that it may lead to a total surveillance society.

  From my point of view, this is probably the worst outcome of this technology.

Surveillance technologies

Most democracies take place in those countries in which the strength of the economy lies in the citizens. These are countries with a great percentage of high-educated people, which remarkably contribute to heighten the position the country has in the world’s economy. For example, by improving the tech and industrial sectors.

Surveillance technologies

Under these conditions, it is beneficial for the governments and economic powers to keep these high-skilled people happy and motivated. Happier people make better workers and in their pursuit of happiness, they are also more prone to buy products, generating profit in both ways. As a result of this symbiosis, citizens have better living standards and are more powerful.

Surveillance technologies

This does not always apply to poorer countries, where it has been thought sometimes more profitable to have the people more controlled and try to enrich the economy by different methods: lowering salaries and rising taxes have been two of them. Provoking a decline in the general well-being of the people.

Surveillance technologies

In the case of the total surveillance model, the data gathered could be matched with the whole digital persona, leading to a society where everybody would need to be afraid of what they do, say or even think, in order to avoid committing errors. As it normally happens in dictatorships.

This situation would weaken the power of the citizens, who would end up having worse living conditions, even if they belong to the group of well-educated people and highly productive workers.

Surveillance technologies. Possible solutions and personal recommendation

From my point of view, the solution to this potential problem would be to regulate the fields in which and the ways how facial recognition can be applied. For example:

- Creating laws to avoid the companies and governments using it indiscriminately.
- Only permitting its use for certain security systems, as in airports.
- Regulating how can be used. For instance, not allowing databases of regular citizens, only of subjects of an arrest warrant.

Surveillance technologies. Possible solutions and personal recommendation

This would minimize the risk of becoming a total surveillance society, and also the room for a possible identity fraud following the hacking of a database.

Should facial recognition systems be regulated?

David Garcia Arias