Human Factors for Apparel and Textile Engineering, Vol. 32, 2022, 39–45
https://doi.org/10.54941/ahfe1001536

CAPABLE: Engineering, Textile, and Fashion Collaboration, for Citizens' Awareness and Privacy Protection

Rachele Didero and Giovanni Maria Conti

Design Department, Politecnico di Milano, Milan, Italy

ABSTRACT

Many private companies and public bodies in authoritarian and democratic states have joined facial recognition technology, used for various purposes. This situation is due to the general absence of a specific regulation that monitors its use. There is no consensus in society regarding the ethics of this technology. Furthermore, there are many doubts concerning the long-term ethical sustainability of facial recognition and its compliance with the law. A problem that emerges from the use of this technology is its obscurity. We do not know who is responsible for the decision automatically made; we do not know how the data is used by those who collect it, how long this data is kept, who can have access to it, to whom it is sent, and how this is used to create a profile. In addition, facial recognition systems are powered by numerous images collected from the Internet and social media without users' permission: it is, therefore, impossible to trace the origin of the data. Consequently, any citizen could be classified, most likely discriminated against, and become the victim of an algorithm. The boundary between security and control is decidedly blurred: many cameras do not respect the privacy of individuals and often harm human rights when they are used to discriminate, accuse, power, and manipulate people. From this discussion on privacy and human rights, it was born first the desire to create awareness, in particular regarding these technologies and the possible issues linked to them. Secondly, it was born the will to create a product that would be the spokesperson for these concerns and allow citizens to protect themselves. On this basis, a collaboration between fashion, engineering, and textile has developed to produce fabric and then garments, which confuse facial recognition systems in real-time. The technological innovation aims to create a system capable of generating adversarial knitted patches that can confuse the systems that capture biometric data. By integrating an adversarial algorithm into their jacquard motifs, the garments prevent the wearers from being identified, preserving their privacy. The adversarial textile is made with computerized knitting machines. Compared to a printed image, knitwear acquires texture, durability, wearability, and practicability. Furthermore, a knitted fabric allows modifying the single yarn material based on the results and performance we want to obtain. These fabrics have been tested on Yolo, the fastest and most advanced algorithm for real-time object recognition. The project was born in New York in 2019; the first experiments with computerized knitting machines were carried out at the Politecnico di Milano in January 2020. The textile was developed in the workshops of the Shenkar College of Tel Aviv. On February 8, 2021, the patent of the industrial process to produce the adversarial knitted textile was filed, with the patronage of the Politecnico di Milano. Today, the research on this fabric and these thematics has carried on within a Ph.D. that combines human-centric design and engineering.

Keywords: Knitwear, Adversarial fashion, Privacy, Human rights, Data science, Facial recognition technology

INTRODUCTION

The first necessity that led to this research being developed derives from the use of facial recognition technology.

Our face represents a sense of uniqueness and peculiarity that will accompany us throughout our lives; it is the most intrinsic data to our person.

Biometric data are personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprint data (Privacy Plan, 2021).

As mentioned, the information collected by this technology belongs to biometric data, like iris images or DNA. However, the facial signature can be captured, and the data collected without the subject being aware of it and without his consent or dissent (Kohnstamm, 2012). This is because cameras are in public spaces or private spaces open to the public. The inability to give consent to the processing of their biometric data related to this technology is one of the problems highlighted by the many movements that declare themselves opposed to facial recognition technology.

One such movement is Amnesty International (2020) which adds that facial recognition technology denies numerous human rights, from the right to privacy to free expression to the right to free association and movement. Furthermore, it states that this technology is discriminatory, particularly against ethnic minorities and at-risk groups, with minors, women, or people with mental problems (Amnesty International, 2020).

Two other critical points concern the diffusion of the technology - 110 states use it[1] - and the uncertainty regarding collecting, storing, and disseminating the data collected (Some, 2020). For the recognition to take place, personal data is collected from massive datasets that draw, for example, from social networks (Information Commissioner's Office, 2021).

Anton Alterman argues that the general right to privacy includes the right to control the creation and use of biometric images of ourselves. He is one of the few critics to raise the issue of informed consent for the management of biometric technology. Fully acknowledging that his policy recommendations run counter to current practices, he suggests that everyone who is asked to voluntarily submit biometric identifiers, should be "1) fully informed of the potential risks; 2) competent to understand the impact of their actions; and 3) under no threat of harm to agree to such an action." (Sutrop, 2010).

The second problem relates to the lack of awareness. Data has become the primary resource of economy, but there is often not enough awareness of this. There is a tendency not to protect our first wealth and uniqueness sufficiently and most people are not in a position to develop an informed opinion on the deployment of facial recognition technology (Pew Research Center, 2019) (Ada Lovelace Institute, 2019).

[1] Facial Recognition Status: In Use. Total Countries: 98.
Facial Recognition Status: Approved, but not implemented. Total Countries: 12.
Facial Recognition Status: Considering facial recognition technology. Total Countries: 13.
Facial Recognition Status: No evidence of use. Total Countries: 68.
Facial Recognition Status: Banned. Total Countries: 3.
(Some, 2020)

This is also due to a lack of means that can raise awareness on the subject, effective and design means, aimed at a wider audience than that of industry scholars, such as jurists and data analysts.

Last problematics regards the scarcity of means that give the possibility to allow the protection of one's facial data.

Given these assumptions, it was felt the need to create a design product that raised awareness of the risks of facial recognition technology. At the same time, it needed to be a product able to protect against this technology.

DEVELOPMENT

The project was addressed as a master's thesis in Design for the Fashion System by Rachele Didero, Professor Giovanni Maria Conti as supervisor.

The research was started at Politecnico di Milano in January 2020 and continued the same year in the laboratories of Shenkar College, where Rachele Didero was on a university exchange.

Initially, background research consisted mainly of theoretical research and anteriority research on existing projects on these issues.

Therefore, the project's uniqueness was established, which had as its objective to create a knitted fabric with adversarial characteristics.

As it is known, there has been a notable development of computer vision techniques in recent years, for example, to reproduce the capabilities of human sight. Within these techniques, the ability to interpret the content of an image itself (Feng, X. et al., 2019). A proposed solution for this problem is based on the so-called adversarial images developed to deceive the most advanced automatic detection systems. Adversarial images, once physically placed near the face of the person exposed to the artificial vision system (Thys, S. et al., 2019), can deceive the algorithm and not allow the user to be recognized as a person (Didero and Conti, 2022).

The adversarial images are complex images, characterized by high definition and a large number of colors; from this element derives the complexity of translating adversarial images in knitwear. In particular, in Jacquard knitwear, the minimum unit of images that can be obtained is the jersey stitch, which performs the function of the pixel in digital images. However, the conversion between pixels and jersey stitches cannot be directly established because the number of pixels in an adversarial image is usually excessive for the size of the machine and, in any case, would result in an image that is too large to be used effectively.

Despite the complexity of the objective, we wanted to obtain a knitted pattern for the properties of the knit itself: increased wearability, comfort, practicality, three-dimensionality. A woven image is more durable than a printed one; it has its texture due to the composition and brightness of each yarn. Finally, knitwear allows modifying the single yarn material based on the results and performance we want to obtain.

It was decided to adopt an experimental and practice-based approach to develop efficient knitted adversarial patches, in which numerous phases of research, development, testing, and modification were defined (Didero and Conti, 2022).

The trials involved various areas, including the composition of the yarn material, the yarns' title, the yarns' coloring, the gauge of the knitting machine, the dimensions of the patch, and the dimensions of the adversarial image (Didero and Conti, 2021).

Furthermore, it included modifying the number of yarn guides used with respective matching colors, the gradation of the yarn in the machine work, the type of back of the jacquard, and the positioning of the patterns on the body (Didero and Conti, 2021).

The practice-based part of the project was divided into two main phases:

- the first phase to obtaining a fabric that is effectively adversarial,
- the second phase for obtaining garments that are adversarial once worn.

The first part was developed over four months (April-July 2020).

The second part was developed over the next four months (August-November).

RESULTS

Protection

The result of the research consists of seven MVPs: two sweatshirts, one t-shirt, three pants.

The seven garments have four different adversarial patterns, each of these patterns, if worn, causes a different reaction to the real-time object recognition software.

Among these algorithms, one of the most widely used commercially is called YOLO (You Only Look Once), available in various versions. We tested the garments with YOLO which is the fastest real time object recognition software.

In the patterns, either nothing is identified, or people or animals such as dogs, zebras, giraffes can be recognized. The animals' confidence percentage varies between 30% and 99%.

The main goal is not to let the faces of people wearing the clothes being inside the software identification bounding boxes. In this way, the subject's biometric data are not calculated, and the facial signature is not constructed.

The tests of the garments with the patterns were carried out indoors (see Figure 1) and outdoors (see Figure 2). This step was fundamental to calculating the effectiveness of the adversarial patterns with different light intensities. From these trials, we can say that the lightening of the environment in which the patterns are worn, and the luster of the yarn are two decisive elements to calculate the textile's efficacy.

Finally, during the tests, the models were asked to wear the garments static and in motion. These moved in the space comprised by the camera lens filming them; they were asked to smile, talk, interact with each other. This step helped verify the effectiveness of the adversarial garments not only in a frontal and static position.

In the conclusive analysis of the collected materials, it was noted that the face of the models with adversarial garments, unlike the models without

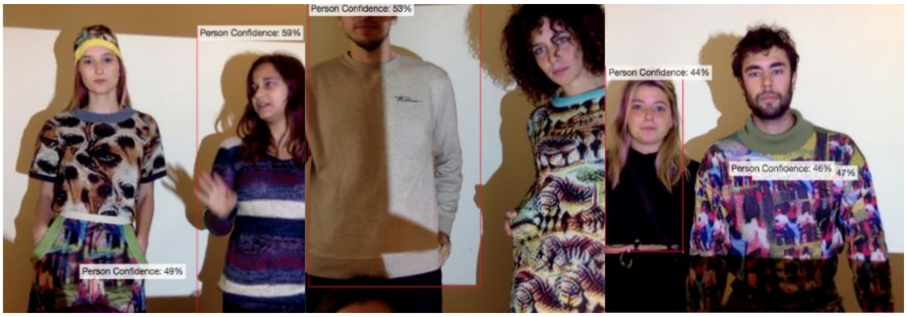

Figure 1: Test with YOLO, indoors.

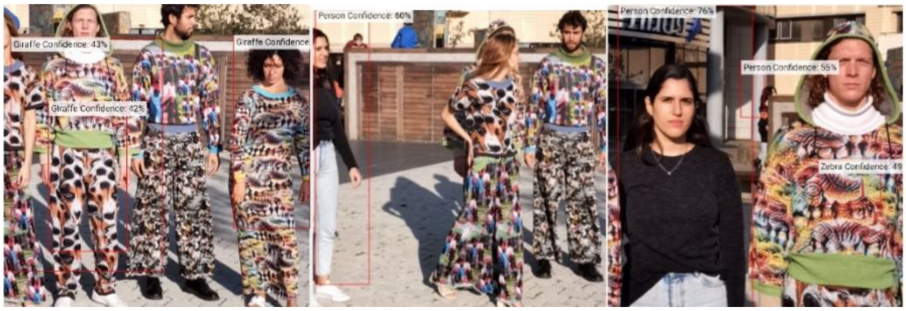

Figure 2: Test with YOLO, outdoors.

adversarial garments, were not classified inside the bounding boxes of the object recognition software; therefore, the experiment achieved its goal.

These fabrics and the garments deriving from them can prevent the detection of the biometric data of the people who wear them in the presence, for example, of the real-time facial recognition cameras.

The patent application of the method to obtain a knitted adversarial image was filed in February 2021 within Politecnico di Milano.

Awareness

This research was carried out to obtain a product that could raise awareness of the emergence of new artificial intelligence technologies. These technologies can undoubtedly represent an opportunity; however, there is a risk that some of them may be misused, thus representing a threat to fundamental rights and democracy.

Based on this reasoning, this project has been called Cap_able, from C_ollaboration between Engineering, Textile, and Fashion, for people's A_wareness and privacy P_rotection.

Cap_able wants to raise awareness of the risks associated with facial recognition technology. In a world where data is a strategic and valuable asset, Cap_able addresses the issue of privacy, opening the discussion on the importance of protection from the misuse of biometric recognition cameras.

It wants to educate on the importance of privacy and human rights and the risks associated with mass surveillance; therefore, it was thought for a cultural and technological avant-garde which becomes a spokesperson for these values.

Cap_able wants to impact society, creating awareness on the issue of biometric data protection that affects most citizens from all over the world.

The necessity to protect the individual from the abuses of new AI technologies is increasingly perceived.

The biometric data of those who wear Cap_able technology is not stored by the large databases in which they are combined with personal data to trace the profiles of each citizen. This project wants to give a tool to decide whether to consent when personal data is collected.

CONCLUSION

The outcomes obtained gave rise to the desire not to end the research but to set new goals in the design and engineering fields.

On the one hand, there is the desire to improve the known technique and obtain new results concerning the security field.

On the other hand, there is the want to continue investigating innovative products, both from a technological point of view and the values they convey.

The target for which this project will expand is that of present and near-future generations.

These are the generations born in the digital age and who need to interface with design products that can meet the needs of everyday life imbued with new technologies.

To continue the research on this field, it is necessary to study the target's feedback on the interaction with the known product.

This feedback will be helpful to keep investigating in the design field and make improvements and study new solutions that meet real needs.

This step aims to combine functionality and ethics and open discussions on themes linked to new emerging problematics.

REFERENCES

Ada Lovelace Institute (2019). Beyond face value: public attitudes to facial recognition technology. https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf

Amnesty International (2020). Amnesty International and more than 170 organisations call for a ban on biometric surveillance. Available at: https://www.amnesty.org/en/latest/news/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/ (Accessed: 13 February 2021).

Didero, R. and Conti, G.M. (2021) *Brevetto per Invenzione Industriale: Metodo per realizzare un tessuto in maglia che riproduce un'immagine avversaria*. Ministero dello Sviluppo Economico Italiano. Patent no. 102021000002729.

Didero, R. and Conti, G.M. (2022) 'Adversarial Knitted Fashion. Method for making a knitted fabric that reproduces an adversarial image'. *Sixteenth International Conference on Design Principles & Practices*. New Castle, Australia, 18–21 January. Presented, awaiting publication.

Information Commissioner's Office (2021) The use of live facial recognition technology in public places. https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

Kohnstamm, J. (2012) Opinion 3/2012 on developments in biometric technologies. Article 29 data protection working party.

Privacy Plan (2021) Article 4 EU GDPR "Definitions". Available at: https://www.privacy-regulation.eu/en/4.htm (Accessed: 10 February 2021).

Some, K. (2020). Which countries allow and which ban ai facial recognition? Analytics Insight. Available at: https://www.analyticsinsight.net/countries-allow-ban-ai-facial-recognition/ (Accessed: 15 January 2021)

Pew Research Center (2019) More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. https://www.pewinternet.org/wpcontent/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf

Sutrop, M. (2010) Ethical Issues in Governing Biometric Technologies. In: Kumar A., Zhang D. (eds) Ethics and Policy of Biometrics. ICEB 2010. Lecture Notes in Computer Science, vol 6005. Springer, Berlin, Heidelberg.