The Executive Master is a unique diploma from École Polytechnique targeted to senior managers that combines technology, innovation management and leadership. This part-time program is designed in modules and allows participants to follow the courses while respecting their professional commitments.

The modules cover various technological and innovation fields such as artificial intelligence, Data Science, biomimicry, IoT, new energies, sustainable development, industry 4.0 or biomedical engineering. The courses are given by researchers working in the laboratories of Ecole Polytechnique and of our partner institutions.

The knowledge acquired throughout the program helps participants to carry out a Team Project and a personal project, the “State of the Art” (SOTA) Report. The objective of the SOTA Report is to produce an updated synthesis on a scientific or technological subject. The document has to be quite short and readable by non-experts.

Over the years, many of these outputs have proven to be both intellectually very stimulating and practically very useful to accelerate the structuration of innovation processes\(^1\). Hence many readers suggested that we make them available to a larger audience.

This SOTA Report is part of a selection we did and for which the authors – now our Executive Master alumni – gave us their authorization to publish and share.

We hope you will enjoy exploring this “treasure”. Do not hesitate to send us some feedbacks or get in touch directly with the authors.

The École Polytechnique Executive Master team

Executive.master@polytechnique.edu

---

\(^1\) Disclaimer: these reports are written under the sole responsibility of their author.
Deep Learning in Facial Recognition: current state and what the Future Holds

**Keywords:** Authentication, Biometrics, Access Control, Deep Learning, Faceprint, Face Recognition, Identification

**Executive summary**

Biometrics as authentication tool has two main reasons to exist: simplicity and security. Using Biometrics as an identification tool, that uses behavior physical characteristics to grant a frictionless and disrupted access to a protected or sensitive environment, is one the main tendencies within modern cybersecurity, protecting from different criminal and malicious activities: fraud, phishing, hacking, terrorism etc. Private companies and public sector embraced this technology yet far from perfection and which require certain improvements. We could see vast opportunities for biometrics. There are plenty of scientific research projects so far to bust the biometric usage based on AI. For example, using video surveillance in dense urban areas, where the speed of analysis could be critical, AI plays a significant role in powering this technology to provide solutions for police investigations. Voice analysis and emotional state analysis for pilot-controller communications during the flight authorization to prevent unauthorized control over the plane or as a compliance supervision tool for brokerage exchange in investment banking to prevent bribery, harassment, or illegal price negotiations. According to Cambridge Dictionary «Facial recognition is a technology that makes it possible for a computer to recognize a digital image of someone's face» (1). This report studies different stages in facial recognition, algorithms which are used and the challenges in the future.
TABLE OF CONTENTS

Introduction ........................................................................................................................................... 3

1. Statistics around facial recognition .................................................................................................. 4

2. Use cases for Facial recognition ........................................................................................................ 5
   2.1 Identification. Who you are? ........................................................................................................... 6
   2.2 Authentication (biometrics). Identity and access verification ......................................................... 6
   2.3 Emotion recognition ....................................................................................................................... 7
   2.4 Specific use cases for emotion Identification ............................................................................... 8

3. Technology description ..................................................................................................................... 9
   3.2 Initial source Initial source to get the Image/video ....................................................................... 10
   3.3 Face detection ................................................................................................................................ 10
   3.4 Face normalization ......................................................................................................................... 12
   3.5 Feature extraction and converting of image into data ................................................................. 14

4. Well known technologies ................................................................................................................ 16

5. Technology advantages .................................................................................................................... 17

6. Facial recognition challenges and future development ..................................................................... 18
   6.1 Accuracy is an issue ....................................................................................................................... 18
   6.2 Vulnerability of biometrics .......................................................................................................... 19
   6.3 Technical challenges improvements ............................................................................................. 20
   6.4 New use cases for the facial recognition ..................................................................................... 21

Conclusion ............................................................................................................................................. 22

Bibliography ......................................................................................................................................... 23

APPENDIX 1 ......................................................................................................................................... 26

APPENDIX 2 ......................................................................................................................................... 28
INTRODUCTION

Facial recognition: this topic became extremely important during the last several years with the development of Machine Learning and Deep Learning. While we are talking about the accuracy of computer technology and the its use cases in different areas in our everyday life, let’s understand why this subject became so sensitive and what is behind it. When we analyze the human capacity to recognize faces, we have 97.53% as an accuracy number for human brains. Moreover, this capability is so important for human’s social life and security that there is a specific area in the human brain (fusiform gyrus) responsible for face recognition only (not for object recognition for example). On the image of the human brain below the area responsible for facial recognition is colored pink.

Source: (2)

The first research on Facial recognition appeared in the 1960s. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson (3) (4) (5) are the first scientists who worked on computer facial recognition using the scanner to map the key facial points: hair, eyes, nose, and mouth. Since that, Facial recognition quality and performance progressed significantly and with a world of digitalization the interest in technology shifted from the pure scientific one and police investigation needs to smart cities, frictionless payments, ID replacement, and even genetic disease diagnostic. In the 1980s the Linear Algebra was used to solve this problem. With computer science development and Machine learning which deploys a network of artificial neurons in the same way as the human brain does, face recognition technology advanced incredibly with many different use cases of our everyday life. Asses to different services with biometric recognition including facial or a fingerprint (like an active usage in Banking services, for example) digitalization takes a big speed. Digital technologies entered our life in absolutely all areas making to it safer and easier.

Why did facial recognition get this significant development during the last several years? What triggered this process? The main reasons, obviously the availability of powerful computers (Moor’s Law in action according to which “that the number of transistors on a microchip doubles
every two years, though the cost of computers is halved”, (6)), the devices and the computers become smaller and more powerful. There are huge bases of outcurves available on the internet, social networks, and on our devices. The quality and the ease of taking and storing pictures allowed us to have Big Data to work on. And one of the most important factors, of course, is neural network development which stays the key tool for face recognition technology.

1. STATISTICS AROUND FACIAL RECOGNITION

Why is this subject so important? In this section, some facts and statistics are proposed to show that this subject is very far to be the only scientific one. The development of facial recognition accuracy and the availability of data raises more questions about ethics and Data Privacy than any other modern technology in the world. Below you can see some examples of wide facial recognition usage globally.

For example, in Singapore, it is deployed at borders passing since 2012, and according to BISCHOFF June 8, 2021 (7) China, Russia and the United Arab Emirates are the countries with the biggest penetration of facial recognition globally, where technology is used by the government even at schools or to identify participants during the protests like in Russia and US.

Here are more statistics, of facial recognition usage which are proposed by Nick Galov (8). We can see the mainstream in service industries, Oracle in it’s Hotel 2025 report estimates the increasing usage of AI and facial recognition in hotel industry: “74% of hotel operators said automating staff recognition with biometrics would be mainstream or in mass adoption by 2025” (9). The global facial recognition market is expected to grow exponentially and according to Grand View Research (10) the size of the market “is expected to reach USD 12.11 billion by 2028” (10). Thanks to AI and DL development, different algorithms deployment, the accuracy in ideal conditions could be at the same level as for humans and even exceed it. The errors producing with new algorithms reduced by 50x (11), facial recognition (FR) systems “can achieve accuracy scores as high as 99.97%” (11)
According to research, governments globally not only actively use facial recognition technology (FRT) for digital ID and police investigations, but “In total, there are now 109 countries today that are either using or have approved the use of facial recognition technology for surveillance purposes”, (12)

The map of governmental FRT usage is shown in the image below. Source: (7).

The technology is use by police forces, at airports, at schools, in Financial Institutions and Banking, in transport system, tracking COVID-19, implemented in some workspace. There are only two countries: Luxembourg, Belgium where the face recognition is still officially banned by their authorities (in Morocco facial recognition was not allowed till December 2020). Many countries on the contrary increased the FRT usage because of COVID-19 in order to track and monitor their population and to reduce the virus transmission.

As we can see, this technology use is part of our everyday life. We wouldn’t concentrate our attention on legal and ethical aspects of the facial recognition, the main task of this report is to better understand how this technology works, what it can detect and what is still a challenge, what would be the next steps of the technology developing and what could be the future applications of facial recognition in the nearest future.

2. USE CASES FOR FACIAL RECOGNITION

When we talk about Facial recognition there are two different use cases which are usually confusing: Authentication and identification. While the use technology is very similar, we still can see that Authentication is not the same thing as Identification. In this study the term Facial recognition is used to cover all use cases.
2.1 Identification. Who you are?

Identification is used to identify people in a crowd, for COVID tracking, and for criminal investigations. It could be also used to provide personalized service in retail such as “Know your customer”. We have a sample (a base of samples) and are looking for the Identification of an individual from a big stream of images. The idea of identification is to identify the criminals and there is no person’s consent required.

The level of false positives here is quite high, which is explained by the conditions when the video or image was taken (the light, the angle, movements, other objects, etc). Some countries prohibit the use of these technologies exactly for ethical and legal reasons, but nowadays especially with the spread of COVID the number of countries where police can use the identification is increasing to prevent the COVID-19. It was successfully used in South Korea, China, Russia, and some other countries and could be also used for other highly contagious diseases.

Another good example is Facebook which identifies your friends on the published picture of an Apple Photo tool, which identifies the same people in different pictures. We can detect: Age, Sex, Ethnic group. Identification is a ‘one-to-many” process (for example using CCTV footage), where the user is unaware of the process, has no control over the privacy, has no influence and doesn’t always get the benefit from (13).

Typical use cases:

- Police investigations
- KYC
- Personalized Customer Experiences
- Personalized marketing
- Hospitality
- Time and Attendance.
- COVID (and other diseases) tracking

2.2 Authentication (biometrics). Identity and access verification.

Facial Authentication uses similar technology, but the use cases are different. In this case, the consent of the user is a required part. Is used to pass the border, for getting a visa, for banking operations, for unlocking iPhone, account protection, in Education to enroll for an exam, etc. In this case, your face is a unique token, we are talking about facial biometrics and Authentication
In the case of authentication, we are taking about faceprint as a human token of access, where the user is aware of the process, understands it, gives his consent, and can potentially get benefits from it (13).

Typical use cases:

- Access control
- Fraud prevention, ID Theft
- Police investigations
- Smart houses and smart cities
- Loyalty programs for frequent clients
- Payments
- Security
- Quick identification of a person in a case of language barrier or health issues
- Identification in case of accident, health problems, death

2.3 Emotion recognition.

This part of the study is much more complex and sensitive in terms of privacy protection and needs not only to detect a face but also to interpret an emotional state, which makes the ML task much more complex, and these studies are much less advanced than a typical facial recognition technology.

Source: (14)

The capacity to “read” the real emotional state on the human face still needs evaluation. The complexity is not only in AI technology development, but even human beings are not able to qualify emotions with 100% certainty. Since pure emotions hardly exist, the mix of them could be tricky even for humans. Age and wrinkles, also influence how emotion would be expressed. Taking these factors into consideration, we understand, that the decision-making based on the AI analysis of emotional state would be still premature. Nevertheless, there are many scientific studies on this topic about different methods use to recognize facial expressions. According to more frequently used classification there are six basic expressions: “anger, disgust, fear, happiness, sadness, and surprise” (15). This technology could
be further used for the public sector, policy issues and loyalty programs, and client satisfaction but from the health perspective, I see the usage is even more important.

Typical use cases:

- Job interview for candidates
- Learning process: to identify the fatigue, the concentration level
- To evaluate the client’s satisfaction or reactions to marketing campaigns.
- Medical cases: Track the mental health and behavior of some patients, evaluate their emotional state, and analyze the bank of patterns. The suicidal attempts and burn-outs in workspaces could be also a subject of investigations
- Human-machine interactions, including robotic maintenance, Automotive industry; the concentration level, fatigue, alcohol/drug influence
- Surveillance for human behavior in the places of people concentration like airports, stadiums, manifestations, crowd management
- Events, entertainment

2.4 Specific use cases for emotion Identification

We need this solution for detection of genetic diseases/disorders (for example, Williams-Beuren Syndrome or DiGeorge syndrome with a success rate detection of 96.6%, (16)) when we don’t need to have an identity but to detect the behavior patterns or physical features which could be less visible for human’s eyes.

Source: (16)

It makes this technology even more important in cases, when symptoms are not as remarkable, but there are some doubts from the medical perspective. Early diagnosis thanks to Facial recognition could be possible according to different scientist (17), and could help many suffering patients including young children to get the treatment they need at earlier stages. It is a fantastic opportunity provided by this technology which probably can bring us much more in terms of diagnosis beyond the genetic diseases but also with other health problems or deviations.
At this moment of FRT development it is still difficult to evaluate the hidden potential in terms of diagnostic capabilities of the tool.

Typical cases (according to different studies of National Human Genome Research Institute (18):

- Human Malformation Syndromes (DiGeorge syndrome, Down Syndrome)
- Noonan syndrome
- Williams syndrome

One of the most advanced solutions which helps to detect, and confirm genetic evaluations is FACE2GENE (19). Deep learning algorithms helps to transcript the photo of the patient into Mathematical formulae which makes the comparisons with different phenotypic traits based on the real clinic data from existing patients. The ML system is constantly learning with new inputs and false positives.

3. TECHNOLOGY DESCRIPTION

3.1 Main stages of facial recognition

If we take two triangles, we know how to compare them: we can compare their sides and their angles. Facial recognition has the same principle based on AI: the system finds the point on the face: a nose, a mouth, eyes etc, calculates the distance between different points, their positioning in relation to each other and based on this information the system can define the person. Each person has a unique facial “configuration” and the special program can recognize faces by seeing thousands and millions of photos and comparing them with the subject being investigated. Thanks to Big Data usage it can learn to define the most significant features to be taken into account. The bigger the volume of Data provided, the more the system becomes “intelligent” and gives more precise result. It is very similar in this regard to the human brain.

What are the main stages for the facial recognition process? We can identify 5 of them (depending on the facial recognition task).
3.2 Initial source Initial source to get the Image/video

We need, first, be able to get the image itself. The first stage is a critical one; since the light, the angle from which the image was taken, the quality of camera’s optic system, the place where the image was taken, other faces presence (in a crowd) will influence the initial data and the performance. A breakthrough in the field of photography, smartphones which allow us to make pictures any moment we want, the quality of CCTV cameras, are the first important step to the accuracy in FR technology.

3.3 Face detection

In contrast to human beings for whom the face detection is obviously an easy task (even a little baby learns it quite fast!) computer needs a specific algorithm to detect human faces and distinguish them from other objects on the image. The main difficulty is that the face is a constantly changing object with speech and emotions, so the math task to detect a face (and identify it afterwards) becomes even more complex. The number of different programs based for example on Python to detect faces in photos and videos is quite impressive and is expanding very fast.

Source: (20)

The image of the face could be set up as a formal description: the shape of the face is oval, on which in a certain place mathematically described we can find a nose in the middle, the mouth in the middle under the nose, two eyes which will have symmetrical positions, etc. We can also define the palette of the skin color, the hair, etc, which would allow the computer to detect the face's presence on the image. The analysis made by Brownlee, Jason (20) shows that the Deep learning process allows us to better detect all faces on the image, without missing any, which was the case in an ML approach, and also the Deep Learning technology allows us to put all key points: the eyes, the
nose, the mouth in a right place. Since the computer is not a human brain, so face detection is purely a math task, where it looks for patterns, specific to a human face. There are many patterns that could be not only human faces specific. Therefore, the algorithm works in several stages. First, the first feature is found, and the system realizes, “There may be a face in this area”. Then it starts looking there for a second sign, and then the third, etc. And finally, it can say with certainty: yes, it is a face!

This will be the starting point for the next stage of Feature extraction when the face will be described by numbers, and all facial parts will be located in a unique way for every single individual. The next stage is to put feature points on the face, which was detected, which would allow afterward to calculate the individual characteristics of the individual face. Different technologies use a different number of these feature points: from 18 to several thousand.

Ideally to recognize the face we need a direct front image of a face looking directly at the camera. Unfortunately, in the reality, it happens not that often. Probably the only place where we are asked to go directly to the camera is the border crossing check. We can see that even the Deep Learning Face Detection technology itself doesn’t allow us to always detect the right placement for the key points on the face, due to the angle of the image. We can see that on the left face points were placed correctly, but on the right one due to the angle, the mouth and the eyes points are slightly misplaced. Since it could give us false results in future face identification and also in the emotional state evaluation, we need to use another layer of face detection to get more relevant results.

Source: (20)

And this is exactly the moment when the Face normalization comes into play.
3.4 Face normalization

When the image is taken for not targeted facial recognition (for example at passport control, when the person could be asked to look directly at the camera), the facial recognition at the airport, in streets, etc. we would need to rotate a non-frontal taken image to have better performance of the recognition. For some purposes, it could be also useful to do a 45° side view.

![Face normalization results](image)

**Figure 1.** Face normalization results under the same identity in unconstrained environment. Face images are under different views across pose, lighting, expression and background. FNM can keep a high-level consistency in preserving identity. On the right of the dashed line is a near-normal face of the same identity.

Source: (21)

Another example of dual normalization (frontal and 45°) from a facial recognition developer GitHub:

![Dual normalization](image)

Source: (22)
On the first row, there is an initial image that was normalized into frontal position (the second row) and into 45° position (the third row).

When we talk about face normalization it is not only the angle of the picture which needs to be normalized but also any facial deformations caused by facial movements, talking, and emotions. Several Scientists from California work on the technology which makes work facial normalization with the usage of Deep Learning. We can see in the image below the normalization of the initial image (the first on the left) to a neutral normalized one (the last image on the right).

![Face Normalization](image)

Source: (23)

In this study, the group of scientists shows how with training methods for a supervised learning system we can get a “normal” face which is not deformed by the processing of a pack of different images from the same person expressing different emotions or even grimaces. The technology allows to transform any face image taken in different conditions of light and with different expressions into a neutral one (which is a necessary tool, since we hardly live our lives with a neutral “passport face”).

We can see in the picture the result of this technology with several stages for the face normalization using the geometry of the face and the knowledge from the different key points locations with different emotions. Emotions change not only the geometry of the face but also its texture.
The main idea of the process is to normalize the geometry and the texture and afterwards to update the output with the DL technology to make it look like a real face and not a synthetic mask. The system learns natural expressions, the skin texture, in other words the appearance of human face putting it into numbers and vectors description.

The main technical issue to overcome is the followings: non-sufficient light and a side angle (which appear mostly in police investigations when the subject was filmed by street cameras and this issue is not relevant in targeting identification as on the border crossing or at the banking counter).

3.5 Feature extraction and converting of image into data

This is one of the main areas of Deep Learning: This is the exact moment when the face is transformed into data, numbers, and digital code. We are getting a faceprint, a unique human “token”, faceprint which consists of a mathematical description of a unique set of physical features and could be used for behavior authentication (the same as fingerprint or digital tokens).
In order to transform the image of a human face into a mathematical formula and numbers we can use different algorithms or even their combination:

- Statistical analysis feature extraction and a hierarchical deep neural network algorithm: trained and not trained. In the case of non-trained model, we develop a deep network from scratch which is a much longer process. “Neurons that selectively respond to faces (face-selective neurons) are observed in various species, and they have been considered as the building blocks of face detection” (26). In the trained models there are already sets of algorithms developed for facial recognition purposes.

- Markov chains (HHM hidden Markov models are used as a part of Markov chain), models use vectors of different lengths. The HMM is comprised of a finite number of states, the transition of state between “initial state probability distribution, and state transition probability matrix”, and also “each state has a set of probability density functions” (27) that are based on hidden and unobservable Markov chains. HHM was actively used for the last 30-40 years in speech and text recognition. In the HMM model for face recognition, the significant areas: hair, eyes, nose, and mouth are processed in the natural order, for example from the top to the bottom. The algorithm based on the Markov chains algorithm allows us to go from the image to a vector. One of the approaches for HMM uses geometrical features of the natural face’s asymmetry which is measured and used afterward for identification. In the image below we can see the schematical view of the human face and an asymmetry in eyes and mouth positioning which is also an individual feature that can be used for recognition.

Source: (28)

- Elastic graphs (Elastic Bunch Graph Matching): “is an algorithm in computer vision for recognizing objects or object classes in an image based on a graph representation extracted from other images. It has been prominently used in face recognition and analysis but also for gestures and other object classes” (29). This method is used for facial rotation (when the face like, it usually happens in the real environment, is not well-positioned in front of the camera, but in a natural movement has an angle for the image taken) it is also used for facial recognition with
emotion changes and expressions. Consequently, this system could be used in a more realistic environment, using CCTV images, for example.

- Wavelet analysis: is a time-frequency analysis method, a very robust one, where the band wavelets are used for decomposition of the face images into frequency levels. This method gives a high level of accuracy, different studies show the accuracy of 98.83% (30) and could also be used for expression recognition. This method is also useful to recognize faces when there are some changes: glasses, beards, and mustaches.

- Principal Component Analysis (PCA), this is an extensively used ML algorithms which has the best accuracy results so far in image recognition. It is a statistical unsupervised method based on factor analysis. The method is to look for the correlation between variables, reducing their numbers, while preserving most patterns and trends, where the image is transformed into a linear combination of vectors (eigenfaces). This process is also called dimensional reduction, so the data set is reduced but the smaller data set still keeps the necessary information.

- Linear Discriminant Analysis (LDA) this algorithm is quite similar to PCA having the similar approach, it is an appearance-based algorithm which is also used for dimensionality reduction as PCA. There are some differences in these algorithms, PCA is an unsupervised method and the LDA method is a supervised dimensional reduction. “LDA is used to find a linear combination of features that characterize or separate two or more classes of objects or events” (31).

There are different algorithms which could be used for facial recognition, usually, it is a combination of at least two of them PCA+HHM for example, but the main idea is to describe the human face with numbers, formulas, and vectors. Depending on the algorithm it uses or not the normalized on the previous stage image to analyze the specific features which are unique for this specific individual.

The next stage of the process is to compare the digital description of the image with a database in order to find matching. For the last 2 years during the COVID epidemic we were wearing masks in all public places, which made the recognition process more difficult. This new challenge forced companies to work on new solutions which would allow making the recognition work in new conditions.

4. WELL KNOWN TECHNOLOGIES

There are various operators that use different algorithms and their combinations that propose different types of solutions.
There are SaaS engines, which are used for more industrial needs: financial institutions, smart cities, payments, security, etc. The main key factors, in addition to the accuracy, are security and user privacy as well as scalability of these solutions, providing customer support, transparency, and ethical and legal compliance.

According to different rankings (Thales provides is one of them) the main big players on the FRT field are the following: “Accenture, Aware, BioID, Certibio, Fujitsu, Fulcrum Biometrics, Thales, HYPR, Idemia, Leidos, M2SYS, NEC, Nuance, Phonexia, and Smilepass” (32).

We can see several popular open-source solutions which are free and used by research (mentioning these sources in their studies). To use these open sources the knowledge of Machine learning and programming language (Python is used very often) are necessary. The list of the most popular is the following: DeepFace, DeepID, VGGface, FaceNet.

In this study the case of Deepface is taken as an example one of the most popular technologies. One of the well-known technologies of Deep learning which allows to normalize the face on the image, analyze it and identify using the database is DeepFace, which is created by Facebook (Meta). This technology is based on advanced deep learning, nine layers deep, neural network, using the immense database of face images (initially for research purposes the volume of the database was 4 million face images). The machine learning process uses 120 million connections between neurons. The software recognizes the same person in two different photos with 97.35 % (+/- 0.25%) accuracy, regardless of how they are photographed: in full-face, in profile, in a good or bad light (33). Humans themselves, by comparison, can correctly match faces in two unfamiliar photos 97.53% of the time, that is, the human recognition mechanism works only 0.18% better than the machine.

5. TECHNOLOGY ADVANTAGES

What are the main advantages of using face recognition technology? Why humans are not good enough to cover this topic as they previously did? We can mention the most significant ones:

- High precision: it means that humans could be replaced by machines without reducing the quality, and in the future, it will even augment the accuracy. It opens a huge possibility to shift some job responsibilities to AI.
• Low risk of cheating, using masks. Modern technologies are capable of better detecting and identifying human faces with additional elements like medical masks, glasses, and beards, then humans, and it gives a big advantage to AI

• Contactless, in comparison to a fingerprint, which in conditions of COVID could be a huge advantage in use.

• It is impossible to make a false faceprint, the fantastic stories from movies, when an character puts on a mask and can trick the identity scan, have no scientific basis. The faceprint couldn’t be transferred to someone else as it can happen with a physical token.

• No necessity to be positioned straight in front of the scanner: it is always preferable to have a frontal-taken image, but modern technologies can normalize the image and still make an identification. The technology is still not perfect, and many factors play a role here: the quality of the optics, lighting, etc. nevertheless the current technology in good conditions can provide the accuracy close to 100%.

• Eliminates the human factor (The officer at the border custom could be tired and miss something and at the same time the personal perception could make (sexists, racist) could make simple verification longer)

• No problem when detecting across ethnic group detection; this is a very important moment. We know that for humans it is much easier to recognize humans from the same ethnic group while people from another ethnic group could look similar (the same face). AI doesn’t have this problem, since it is trained for all races and has no personal perception.

6. FACIAL RECOGNITION CHALLENGES AND FUTURE DEVELOPMENT

6.1 Accuracy is an issue

If we want to define facial recognition in one word, we will talk about accuracy which is the main issue here. “A facial recognition system can achieve up to 99.97% accuracy” (11). Of course, when we talk about these numbers like in any other scientific experiments, we are taking the ideal conditions which could literally only exist in the laboratory with perfect light, angle of the camera, the subject never closing his eyes or looking away from the camera, no movements, no other objects are influencing the experiment. In a real-life situation the statistics are slightly different and according to (11) is about 90%. To replace PIN codes and passwords Biometrics should work in 100% cases which is still not the case. Weather, light, noise, and other external conditions could interfere and compromise the input.

One of the Facial recognition’s challenges for identification and Authentication purposes is the same as for human eyes: the distinguishing of twins. Face recognition algorithms tested about 10
and even 5 years ago were not yet capable to distinguish twins. Interestingly the AI had difficulties not only with identical (monozygotic) ones, where humans a having the same issues, but also same-sex fraternal (dizygotic) twins or very similar brothers or sisters. Even if all identical twins have always unique fingerprints (neither faceprint, voice, retina, and iris) but there for crimes and fraud, for police investigations that could be not enough. The CCTV footage with modern technologies can’t say with certainty which one of the twins was filmed. Unfortunately, according to statistics, the twins, which have the high degree of resemblance, have much more tendency to commit fraud or crime (even kids use their similarity to trick their parents or teachers in schools). However, even if theoretically the faceprint would be different for twins, in the real circumstances we don’t always have an opportunity to get fingerprints, on the other had having CCTV records is much easier. Unfortunately, we usually have the image with noise facial expressions, movements, etc. and because of twins' similarity, the distinguishing process is still almost impossible (for example even no monozygotic twins can unblock a face ID on the iPhone). So, fingerprints and iris biometrical identification stays still in priority. (34)

The main idea of using the face recognition tool is to make the process of identification faster, easier, and frictionless. Therefore, if we want this tool to be used as a full/partial replacement of other more traditional tools such as ID cards fingerprints (which are already an advanced biometric digital identification tool widely used in phones, border crossing, to control an access area, background check and for criminal cases), the accuracy is a key.

We need to take into consideration that face recognition as a part of behavior identification, including voice, mouse movements, etc. is much more susceptible to personal changes such as illness, weight changes, traumas, stress, emotional instability, and other personal circumstances would change the normal behavior.

6.2 Vulnerability of biometrics

We can change the PIN code and a password, but we can’t change our unique biometric feature, our face is a unique “token” in the form of a human face. Consequently, the consequences of stealing the Data for the purpose of its malicious usage are extremely serious. The storage of the Data, privacy and personal rights, technology manipulation (cybercrimes), ID theft, and potential errors (false positives) this is not an exhaustive list of potential risk. While the technology continues to develop, the main risk is on the legal and ethical side.

Nowadays, less time is needed to create and train more powerful a facial recognition algorithm, accessibility in terms of required recourses and social media penetration in everyday life caused
a lot of privacy risks. Literally, almost everyone with some coding knowledge and computational power can train powerful facial recognition models using Python for example.

Images posted on social media and zoom calls could be used to search for personal information about my family, current location, etc.

Source: (35)

Clearview is a search engine for faces. You upload your face into the system and find all public material (even on social media which were public but not public anymore) that matches this particular face. This tool searches in billions of photos with high accuracy and around 0% of false positives. The difference is that they work really with Big Data, all available police data, and social media as well, as surveillance camera footage. (11)

6.3 Technical challenges improvements

- Accuracy and reducing false positives (10 million arrests annually based partly on facial recognition). Nonetheless, in the ideal conditions with lighting and frontal position the error rate is only 0.1%. While in the accuracy level for an individual walker on the street with outdoor footage is “ranging between 36 percent and 87 percent, depending on camera placement” (11)

Consequently, the facial recognition usage for Authentication (payments, custom, for example, is more relevant.

- Handling harsh lighting condition remains a challenge

- Image normalization still needs to be improved, since the positioning of the face and the angle has so many varieties, the normalization still doesn’t give the perfect result in 100%

- Occlusion: glasses, masks (COVID situation was a big issue for the future development of the identification process when more than a half of the face was hidden), beards, artificial makeup like for football supporters for example, when the system can’t even detect the face in the crowd and this could be an issue for police investigations, for example.

- Serious changes in the weight (gain/loss) of the individual. Several scientific researchers emetically proved that serious changes in the body weight “significantly reduce the matching accuracy of the face recognition system” (36). The same observation noticed users of FaceID,
that after losing weight, FaceID should be retrained to learn a new face of the same user. We can suppose that serious diseases could also influence the accuracy and surely the age and the wrinkles. By default, according to medical data, the bone structure of the skull is definitely formed by the 13th anniversary, nevertheless, the empirical studies prove that the current technologies still need improvement.

- Correct detection of the emotional state
- The skin color which can change with normalization of the image due to the lighting conditions
- Difficulties in work images which we transformed with different artistic filters (like Instagram bloggers) are difficult to normalize and consequently to use for identification.

- There is an astonishing fact that Face-scanning solutions shows us 35 times less errors in identification of white male, including gender identification, than in identification of a black female, (37). Indeed, according to (8) the problem is in Data volume which is not enough for Black females. That’s why to reduce errors the algorithms to recognize, for example, Asian faces should be trained on the Asian database. EU proposals “for regulatory frameworks for facial recognition include requirements that training data reflect all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination”, (38).

6.4 New use cases for the facial recognition

There is no doubt that, despite the vulnerability issues of data storage, and the risk of malicious usage of faceprint, the technology will continue to develop in terms of accuracy of detection. So, more use cases will be available. The health and diseases diagnosis topics will be probably the most active in scientific investigations while smart-cities, payments, and retails can already get a profit from the modern level of existing technologies. Emotional state detection, that is for now the subject which has a lot of antagonists from regulation and ethical point of view could bring on the significantly new level the crowd and the crisis management, not only the emotional state analysis but also the prediction technologies which can prevent catastrophic event on the big scale but also in everyday life, like car driving accidents, suicidal attempts, etc.
CONCLUSION

The facial recognition technology based on AI and DL is one of the most sensitive and controversial subjects concerning AI development and its influence on human life. Since the first attempt to use computers to recognize faces 60 years ago technology had made fantastic progress. New algorithms and their combination are constantly being put forward by researchers and all IT giants like Meta, Amazon, and Microsoft have laboratories devoted to facial recognition. At the same time, this technology brings a lot of social anxiety, about how technical improvements in our life would influence privacy and human rights.

Based on the legislation and even more on the cultural values in different countries (in France this topic, for example, is much more sensitive than in Singapore) the development and usage of this technology will be different. The usage of facial recognition requires clear regulations, usage, the data storage, all these aspects should be transparent and clear. In this case, the technology could be used and improved based on empirical feedback. At the same time, it is highly important that the legislation wouldn’t play a limited role in the development itself.

The future development in the technology itself is mostly in the accuracy field, how can the AI reconstruct the true image of the individual, from a poor-quality image. It will certainly progress with the quality camera improvements and probably with the capacity of cameras to capture more data, which could be analyzed and used for the training.

Another direction for significant improvements in facial recognition will be the computer processing itself. The clusters of computers, which are used now to process the Data and transfer the data through the network, bring input-output restrictions and limit processing speed.
BIBLIOGRAPHY

13. Star Link, Indian Manufacturer of Biometric Solutions.


23. KOKI NAGANO, HUIWEN LUO, ZEJIAN WANG, JAEWOO SEO, JUN XING, LIWEN HU, LINGYU WEI, HAO LI. Deep Face Normalization. s.l.: Association for Computing Machinery, 2019.


29. Scholarpedia.


34. Zhenan Sun, Alessandra Aparecida Paulino, Jianjiang Feng, Zhenhua Chai, Tieniu Tan, Anil Kumar Jain. A Study of Multibiometric Traits of Identical Twins. 2010.


51. Templeton, Graham. Facebook is working on ‘deep learning’ neural networks to learn even more about your personal life. September 23, 2013.
APPENDIX 1

Privacy protection. AI and ML based solutions of “anti” facial recognition

Of course, the privacy of the data and easy access to personal faceprint which potentially could be used for illegal purposes cannot be ignored by product developers who are working in parallel with Facial recognition technologies looking for protection of images published on social media. One of the opposition movements to facial identification is called Fawkes. One of the examples is the D-ID startup which with the slogan “same image. No face print” developed a program that can block facial identification. The program changes your image on the photo, so it keeps similarity but makes the recognition by facial recognition software impossible.

The face has PII (personally identifiable information) and the idea is to keep the same image for human eyes so they don’t recognize the difference but to make the image nonidentifiable by AI. This solution suggests protecting privacy and to lower the risk associated with breaches, face leakage and malicious usage.

Sources : (41), (42)

The AI doesn’t see the same person, while for the human beings it is still the same one. Humans don’t really see any differences:
Another usage of this technology in a video by replacing the real individuals with their PII with another image, which have the same characteristics (age, sex, ethnic group, etc) but the image will be not the same. It would allow sharing the video without any GDPR concerns.

The warning statistics concerning the data availability is one of the reasons for creating this “anti facial recognition” technology which from the scientific perspective itself could be an interesting subject for studies:

- “Market leader Facebook has reached 2.4 billion monthly active users, while its photo-and video-sharing app Instagram has over one billion monthly active accounts” (44)
- “Facebook: More than 300 million photos get uploaded per day” (45)
- “Each day 95 million photos and videos are shared on Instagram” (46)
APPENDIX 2

Legal and ethical aspects in different regions

To reduce the unauthorized usage of faceprint, fraud and to protect the privacy data and illegal use of the emotional state detection all countries work on the law reinforcement and on the transparency requirements for face recognition. Some countries allow more extensive usage like China or Singapore, some of them like Belgium and Luxembourg banned facial recognition usage in their territory. In some states of the U.S. local governments also passed some law restrictions on the technology use cases. In European Union, biometric Data, including the Data which is generated by facial recognition software is the subject of GDPR regulations. In addition to consent requirements to gather and use personal data, there is also a risk of breaches, stealing the Data, and its malicious usage. In Europe the European Commission introduced its Proposals, and it extensively works on the rules and AI and particularly facial recognition uses cases which could be allowed in the EU territory. The Proposal from April, 21st 2021 “aims to steer AI uptake to reach a high level of protection of public interests, including health, safety, and fundamental rights”. (39)

According to a European Commission statement, “FRT is a sensitive tool for LEAs. LEAs are executive authorities and have sovereign powers. FRT is prone to interfere with fundamental rights – also beyond the right to protection of personal data – and is able to affect our social and democratic political stability.” (40)

The regulation is different in each country, but it is obvious that it will have an influence on technology development and its broadening usage.