D-ID

The EU General Data Protection Regulation (GDPR) and Face Images

De-identification of face images in corporate databases for the enhancement of privacy while preserving visual similarity

WHITE PAPER

www.d-id.com

Introduction

The GDPR (General Data Protection Regulation), taking effect in May 2018, introduces strict requirements for personal data protection and the privacy rights of individuals. The EU regulations will set a new global standard for privacy rights and change the way organizations worldwide store and process personal data. The GDPR brings the importance of preserving the privacy of personal information to the forefront, **yet the importance of face images within this context is often overlooked**. The purpose of this paper is to introduce a solution that helps companies protect face images, to strengthen compliance with the GDPR. D-ID™ is the first to fill the gap between the regulatory requirements and the face image protection solutions currently available, while ensuring data utility through preserving the visual similarity.

Our Face is our Identity

Our face is the most fundamental and highly visible element of our identity. People recognize us when they see our face or a photo of our face.

Recent years have seen exponential increase in the use, storage and dissemination of face images in both private and public sectors - in social networks, corporate databases, smart-city deployments, digital media, government applications, and nearly every organization's databases.

The Rise of Face Recognition

Significant developments in face recognition technologies and applications have and continue to emerge in the market. With the advancements in AI, face recognition algorithms have become more accurate than humans. More and more organizations are using people's faces as identifiers, when crossing border controls, withdrawing cash or accessing smartphones. Governments worldwide already apply face recognition for different use cases. In addition, financial services like Mastercard and retail chains such as Tesco and Walmart have incorporated face recognition solutions.

Concerns & Risks

It is common knowledge that organizations and governments are storing our personal data. A recent example is the case of Facebook and Cambridge Analytica. Due to a loophole in the privacy protection, data of 50 million Facebook users were exposed to the consulting firm which helped Trump's election campaign. China collects personal data on payment credibility, social behavior and purchasing habits to rank its citizens. As part of this data, face images are critical and when processed by face recognition systems serious privacy concerns might be raised.

The Russian app FindFace applies face recognition with the intention for users to find people on the social network VKontakte but was actually used to harass people by exposing very personal details. Earlier this year, the biometric database of India was leaked and unauthorized access to personal information of India's citizens enabled.

Face images are particularly prone to misuse. Anyone with access to the images can gather personal information and hack into accounts. Stored face images pose the risk of misuse, unauthorized tracking and identity theft. With the growing use of face images, the databases get larger and consequently, also the risk of hacking and violation of privacy rights grows. This troublesome reality signals the end of our basic public anonymity as we know it. **This is one of the many reasons why face images are now considered sensitive personal information**.

Face Images as Sensitive Date under the GDPR

Recent regulatory initiatives, specifically the GDPR, have recognized these concerns and risks, and further highlight the importance of protecting personal data.

Sensitive data is a special category of personal data that is subject to additional protections. According to the GDPR, biometric data constitutes a 'sensitive' category of personal data. The GDPR particularly states that the processing of biometric data for identification purpose is prohibited. Processing is only justified if explicit consent of the relevant person exists, specific legal obligations apply or if the processing is required for reasons of public interest. The GDPR defines biometric data as:

*'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, **such as facial images**'*

Face images are categorized as sensitive data under the GDPR and need to be protected.

De-Identification and Data Utility

De-identification is a method for privacy protection and describes the process of removing personal identifiers of certain data. The de-identification of face images is becoming a critical need in order to protect personal information and prevent fraudulent use.

Currently available de-identification techniques provide a range of tools – from relatively weak techniques that can modestly reduce privacy risks, to strong techniques that can effectively eliminate most or all privacy risk. But a common trade-off is that, the stronger the applied de-identification, the greater the loss of data utility and value.

When considering face image de-identification, a crucial factor that comes into play in many scenarios is the stringent requirement regarding the preservation of the visual naturalness. Current anonymization methods include blurring, pixelation, face swapping, deterioration, quality reduction and K-SAME. However, these techniques dramatically affect the visual similarity of the face image compared to the original. Ideally, the de-identified face image remains highly similar to the original one in the eyes of the human viewer in order to enable seamless use of the image for various purposes. To preserve the visual naturalness and ensure data utility, a large set of facial attributes needs to be maintained. However, that increases the vulnerability to unauthorized reuse of the images.

The goal lies in creating win-win solutions, compared to current approaches where unnecessary trade-offs are made, enabling both privacy and data utility.

D-ID's Innovative Solution

D-ID™ is a ground-breaking technology that protects facial images from facial recognition technology. The product modifies images to prevent the identification by automated face recognition systems while preserving the identification by humans. Moreover, it is designed in a way that makes it difficult to be overcome by AI.

On the contrary to the current anonymization methods mentioned above, D-ID™ uses only modification methods which were specifically tailored to be difficult for the human eye to distinguish between the original and the altered image. The visual naturalness is preserved, and seamless use of the image is enabled. While the modified face image is almost identical to the original, it is resistant to facial recognition systems, effectively protecting it from misuse.

Conclusion

Global organizations which store and process face images, collected in corporate databases, shared on social media or used for identification and authentication purposes, need to implement solutions that ensure the protection of privacy, as well as meet data protection requirements to comply with the GDPR.

By changing the biometric data from sensitive to non-sensitive, D-ID protects face images from face recognition technologies and their risks while preserving the visual similarity of the image.

Thus, D-ID facilitates organizations' compliance with the GDPR. D-ID's privacy enhancing solution reduces the risk of fines and lawsuits and relaxes notification requirements in case of a data breach. D-ID helps companies implement the 'Privacy by Design' concept of the GDPR, which promotes privacy and data protection from the start, integrating appropriate privacy principles into the development process. Furthermore, D-ID enables companies to apply the 'Right to be Forgotten' concept and balance between privacy and data utility. At the moment, D-ID™ is the sole available solution.

Contact Us:

sales@d-id.com

www.d-id.com