UBINODES

RESEARCH: FACIAL RECOGNITION

Research: Facial Recognition

The use of facial recognition software is growing, with many companies integrating it into their operations. Understanding how facial recognition software works is essential for grasping potential responses and actions that can be taken in relation to its use.

Disclaimer: We are not affiliated with the mentioned companies, and this article presents solely independent findings. The provided links are for your convenience, and there is no affiliate marketing involved.

How we write our reviews: To ensure an impartial and comprehensive review, all apps undergo testing in the following ways:

• In real-time, applied to actual projects.

• Evaluated by diverse team members situated in different countries.

• Tested on various devices and operating systems.

• Assessed for a minimum of two weeks, with an average duration of four weeks.

• The article undergoes peer review by team members before being submitted to the app developers for the final review.

Contents of this article.

1. What is Facial Recognition?

Facial recognition software identifies individuals through digital images. This analysis system is used by various companies, from security systems and computer companies to social networks. The use of facial recognition software is continuously expanding, with many different companies adopting this technology.

2. How does the Software Work?

Understanding how facial recognition software works is crucial to understanding potential responses. When someone's photo is uploaded to a database, such as on Facebook or captured by a security camera, their facial features are quickly compared to other images in that database. For instance, Facebook can identify similar features and show additional photos of

a person when a new one is uploaded. This process involves analyzing common facial features like shape, depth, color, and detailed characteristics to make matches with other pictures.

3. Commonly Used Facial Recognition Software.

Many major corporations, including Facebook, use facial recognition software for various purposes. Facebook's DeepFace technology, which captures microscopic details from camera lenses, boasts an impressive 97 percent accuracy in recognizing faces, surpassing the FBI's Next Generation Identification system, which has an 85 percent accuracy rating. Despite differing privacy laws across countries, companies like Facebook appear to employ this technology without public awareness. Facebook claims it uses facial recognition for connectivity purposes, but concerns arise over potential undisclosed data usage, particularly in targeted marketing.

Google has come under scrutiny for its facial recognition software integrated into Google Photos, showcasing advanced programming capabilities, including the identification of animals. In the U.S., Google's Arts and Culture app, which lets users match their selfies with artworks, raised privacy concerns. Although Google claims the data is not saved, it is transmitted to Google's system for matching, prompting privacy discussions.

Apple has incorporated facial recognition software to unlock its devices, showcasing an unprecedented level of precision that mitigates hacking concerns. Meanwhile, casinos employ facial recognition to track gamblers, ostensibly for managing gambling addiction, yet the potential for other uses, such as monitoring high spenders or card counters, remains.

Beyond entertainment, bars use facial recognition to verify patrons' drinking age, helping to remove underage individuals, including those with fake IDs. While concerns about misidentification exist, the software's accuracy is primarily suited for security and law enforcement applications in crime-related incidents rather than commercial monitoring.

4. Why it is used?

Facial recognition software, which originated in the 1960s, has gained prominence in recent years. Initially used for security purposes, its goal was to match criminals captured on security cameras with mugshots and identification cards. The rise of social media and widespread smartphone use has further accelerated its adoption. Social media platforms enabled constant photo-sharing, while smartphones allowed for instant uploads, contributing to the technology's widespread use.

The rise of individual photography and selfies, especially within millennial culture, has flooded online platforms with a large number of facial images. This abundance of photos has made it easier for companies to extract user images for marketing and commercial purposes. By analyzing profiles and linking faces with social connections, locations, and activities, companies can create personalized marketing profiles without individuals necessarily being aware of it.

5. Safety Concerns.

In the past, facial recognition was mainly used to apprehend criminals, with privacy and safety concerns often overlooked. These images, sourced from security footage, were primarily used to track individuals posing potential threats to society. However, with the advent of the internet and social media, safety concerns have escalated. Companies now have the ability to track personal preferences, locations, decisions, and even identify people in your social circle, creating detailed profiles for targeted marketing.

Beyond marketing, governments can access these profiles and exploit the information to control individuals. For instance, in Shenzhen, China, facial recognition cameras identify jaywalkers, publicly shaming them on screens to enforce compliance—an erosion of public anonymity reminiscent of an Orwellian dystopia.

Online platforms like Alibaba allow users to "pay with a smile," using facial recognition for transactions. Facial recognition is also used on smartphones and computers for unlocking devices. While marketed as convenient, these technologies also collect data about users' daily lives. Companies use this data for marketing purposes to understand habits, social class, and purchasing behaviors. In stores, digital tags adjust prices based on customer profiles, potentially influencing consumer behavior.

Furthermore, governments that have access to this data can exert control, potentially limiting personal choices. Authoritarian states may manipulate personal information to make decisions for individuals, eroding their autonomy. Some facial recognition software even attempts to identify users from behind, which raises security concerns. For individuals living in countries that suppress diverse sexualities, being identified through such software could lead to trouble, even for actions not officially recorded.

6. Alternatives and Solutions.

As facial recognition technology's pervasive influence grows, evading its reach may seem challenging, but there are practical measures to safeguard yourself against it. Here are some suggestions, ranging in difficulty but all aimed at enhancing your privacy:

1. **Social Media:** To protect yourself against facial recognition, start by managing your social media presence. Remove any existing pictures of yourself and avoid uploading new ones. Instead, opt for images of landscapes, animals, or objects to obscure your facial identity while still expressing your interests.

2. **Unlocking Devices:** Avoid using facial unlock features on devices like phones, tablets, and computers. Opt for alternative unlocking methods to maintain a discreet link between you and your devices.

3. **Payments:** Avoid using facial payment options offered by various companies. Despite their convenience, the compromise in terms of privacy is too high a price to pay.

4. **Camera Finders:**Invest in a camera finder that alerts you to nearby security cameras. This gives you a chance to conceal your face before passing by, helping you avoid being unknowingly captured on camera.

5. **NIR LEDs:** Invest in a camera finder that alerts you to nearby security cameras. This gives you a chance to conceal your face before passing by, helping you avoid being unknowingly captured on camera..

6. **Masks:** In places where facial recognition is a concern, consider using masks for added anonymity. Options include surgical masks that cover the lower part of your face, ski masks, or even more elaborate prosthetic masks that mimic someone's appearance without revealing your true identity.

7. Conclusion.

As facial recognition software continues to proliferate, strategic considerations in evading it become imperative. Your face is increasingly identified in all facets of your personal life, leading to a relinquishment of privacy and autonomy. Exercise judicious use of your facial data and remain vigilant. The prevalence of this software exceeds our collective awareness.

8. References.

- **Facial recognition system. En.wikipedia.org**
  https://en.wikipedia.org/wiki/Facial_recognition_system
- **Face Recognition Software: Best-in-Class Enterprise Facial Recognition Security Platform. FaceFirst Face Recognition Software.**
  https://www.facefirst.com/
- **Biometric Facial Recognition - FindBiometrics**
  https://findbiometrics.com/solutions/facial-recognition/
- **Top 8 Ways Facial Recognition Software is Being Used Today - Tech Guru, LLC**
  https://www.techguruit.com/top-8-ways-facial-recognition-software-used-today/
- **Facial Recognition Applications - Security, Retail, and Beyond: TechEmergence.**
  https://www.techemergence.com/facial-recognition-applications/
- **Revealed: how facial recognition has invaded shops – and your privacy the Guardian.**
  https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto
- **Hannah Williams. How is facial recognition used? Techworld.**
  https://www.techworld.com/picture-gallery/tech-innovation/how-is-facial-recognition-used-3668674/

- **Home Garden. How Facial Recognition Systems Work. HowStuffWorks.** https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition4.htm
- **Understanding Facial Recognition Software. The Franklin Institute.** https://www.fi.edu/understanding-facial-recognition-software