ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

Facial Recognition Technology: A Comprehensive Overview

Li Qinjun*, Cui Tianwei, Zhao Yan, Wu Yuying

School of Electronic Information and Artificial Intelligence, Shaanxi University of Science & Technology, Xi'an, China
**Corresponding author*

Abstract: *This paper provides an extensive review of facial recognition technology, tracing its historical evolution, exploring its functioning and applications, discussing the challenges it presents, and contemplating future prospects. The technology's inception and advancement are traced from its early stages to the current state, highlighting the key developments that have shaped its progression. An exploration of various types of facial recognition systems, including 2D, 3D, and thermal, underscores the diversity and complexity of this technology. A detailed explanation of how facial recognition works is provided, outlining the processes of data acquisition, face detection, feature extraction, and matching. We further delve into the broad array of its applications across multiple domains, such as security and surveillance, smartphone authentication, social media, healthcare, and retail. Despite the impressive benefits and applications of facial recognition technology, it also presents notable challenges. These include accuracy concerns, privacy and ethical implications, and the need for comprehensive regulatory frameworks. The paper concludes with a forward-looking discussion on the future of facial recognition technology, considering potential innovations and growth predictions. This review provides a comprehensive understanding of facial recognition technology, underscoring its relevance in our digitally driven world and the implications it holds for the future.*

Keywords: *Facial recognition, Applications, Challenges, Future prospects*

1. Introduction

Facial recognition technology has rapidly become one of the most significant technological advancements in the 21st century, marking an era where machines can identify or verify individuals simply by analyzing patterns based on their facial textures and shapes. The usage of this technology spans a broad array of applications, ranging from security[1] and law enforcement[2] to social media[3] and healthcare[4], revolutionizing how systems authenticate identity and how we interact with our devices and services.

The technology of facial recognition operates by comparing selected facial features from a given image with faces within a database. This method of biometric identification uses relevant features from a human face for identification purposes, providing a non-contact process that is typically highly effective. Though it may seem like a recent innovation, the development of facial recognition technology traces back several decades.

The significance of facial recognition technology lies in its transformative potential. It is poised to profoundly influence sectors such as security, retail[5], banking[6], and even entertainment[7], with new applications being discovered constantly. These applications have the potential to make our lives more convenient, secure, and personalized. As with any technology, the rise of facial recognition also introduces several challenges, such as issues related to privacy[8], ethics[9], and regulatory compliance[10].

In this comprehensive review, we aim to shed light on the various aspects of facial recognition technology. We will explore its history and evolution, delve into how it works, illustrate its diverse applications, and discuss the challenges and limitations it presents. We will also look towards the future, contemplating the potential developments and innovations that could shape the landscape of facial recognition technology.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

2. History and Evolution of Facial Recognition Technology

Facial recognition technology has a long and varied history that has spanned decades, evolving through distinct stages and developments that have led to the sophisticated systems we see today.

2.1. Early Stages of Facial Recognition

Facial recognition technology's origins trace back to the mid-20th century, though not in the digital form we know today. In the 1960s, Woodrow Wilson Bledsoe, an American mathematician and computer scientist, initiated a project on manual facial recognition[11]. Bledsoe's system required administrators to manually input the coordinates of facial features like the eyes and mouth on photographs. The data was then used to compare and identify faces in the database, marking the early efforts to automate facial recognition.

The idea of automated facial recognition started gaining traction in the 1970s, thanks to advancements in pattern recognition and computer technology. Goldstein, Harmon, and Lesk used 21 subjective markers, including hair color and lip thickness, to automate face recognition[12]. However, the technology was far from perfect and was constrained by technological limitations and the lack of an adequate database.

2.2. Key Developments in Facial Recognition Technology

The 1980s and 1990s saw considerable improvements in facial recognition technology, thanks largely to advances in computer vision, machine learning, and computing power. One of the pioneering systems during this era was developed by Sirovich and Kirby (1987), who demonstrated that fewer than 100 values were required to accurately code a suitably aligned and normalized face[13]. This led to the use of principal component analysis (PCA) for facial recognition, popularly known as eigenfaces.

Principal Component Analysis (PCA) is a widely used method for data dimensionality reduction and visualization. It involves a linear transformation that converts high-dimensional data into a lower-dimensional representation while retaining the essential characteristics of the data. PCA achieves this by identifying the principal components of the data and projecting it onto a new feature space.

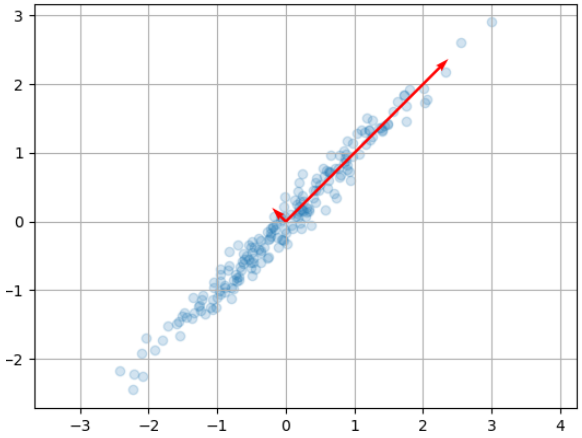

Figure 1: Principal Component Analysis.

Figure 1 is a two-dimensional dataset with data points exhibiting a certain distribution. By applying PCA, we can determine the most significant direction in the data, known as the first principal component. This principal component represents the direction of maximum variance in the data and captures the primary variation. The second principal component in PCA is orthogonal (perpendicular) to the first principal component. It represents the direction of maximum variance in the remaining variance of the data. By selecting an appropriate number of principal components, we can reduce the dimensionality of the data from a higher-dimensional space to a lower-dimensional space. In the depicted diagram, the data points are projected onto the new principal component space, resulting in better separation of the data. This aids in gaining a better understanding and visualization of the data. PCA allows us to capture the essential features of the data and reduce its dimensionality, which is valuable in various data analysis and machine learning tasks.

In 1991, Turk and Pentland further developed the eigenfaces method[14], making it computationally

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

efficient for large databases. This breakthrough led to more accurate and efficient facial recognition systems, setting the stage for the commercial use of the technology.

The 1990s also witnessed the development of other notable facial recognition techniques, such as the Fisherfaces[15] method by Belhumeur, Hespanha, and Kriegman (1997), which enhanced recognition performance under varying lighting conditions and facial expressions.

Fisherfaces is a face recognition method based on Linear Discriminant Analysis (LDA). It is developed as an improvement over Principal Component Analysis (PCA) to enhance the accuracy of face recognition. Unlike PCA, Fisherfaces takes into account the class information of the data while performing dimensionality reduction. It selects the optimal projection vectors by maximizing the between-class scatter and minimizing the within-class scatter, ensuring maximum separation of data points between different classes.

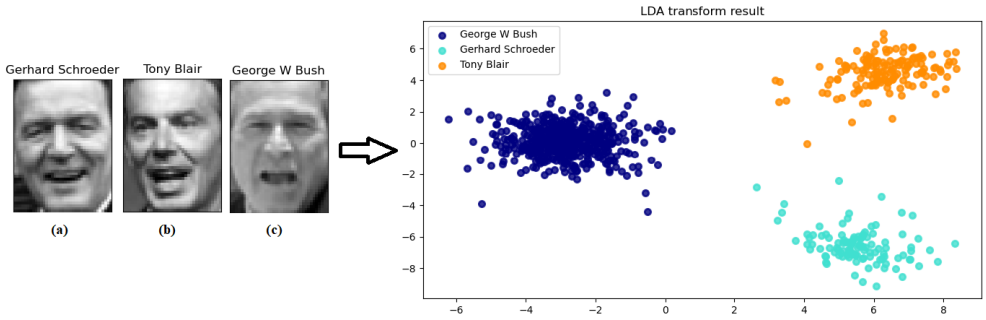

Figure 2: Feature extraction using Fisherfaces.

Figure 2 is an example of face recognition with face images of three different individuals (a, b, c). By applying Fisherfaces, the algorithm first projects the face images of each individual onto a lower-dimensional space. Then, by calculating the mean and covariance matrices of the projected data, it determines the optimal projection direction to maximize between-class scatter and minimize within-class scatter. Through Fisherfaces, we obtain the optimal projection vectors for face recognition. During the testing phase, we can project new face images onto this lower-dimensional space and compare them with the projections of the training set to determine their corresponding classes. Fisherfaces has wide applications in face recognition, particularly on relatively small datasets. By considering the class information and reducing the differences between different individuals, it improves the accuracy and robustness of face recognition.

The emergence of local feature analysis in the late 1990s and early 2000s brought forth another evolution. Instead of analyzing the whole face, researchers began focusing on local features like the eyes, nose, and mouth. This approach, combined with the development of 2D and 3D recognition techniques, significantly improved the accuracy of facial recognition.

2.3. Current State of Facial Recognition Technology

The 21st century brought with it a seismic shift in the capabilities and application of facial recognition technology. The integration of artificial intelligence, particularly deep learning techniques, has been transformative.

DeepFace[16], developed by Facebook in 2014, represented a key milestone in this regard. DeepFace leverages a deep learning neural network model to identify human faces in digital images with a high degree of accuracy, nearly as effective as the human ability to recognize faces.

The primary goal of DeepFace is to enable large-scale face recognition, accurately identifying and matching faces among millions of users. The core idea is to transform facial images into high-dimensional feature vectors and compare the similarity between these vectors for face matching.

The workflow of DeepFace involves the following steps:

1) Preprocessing: The input facial images are initially standardized, including alignment, scaling, and rotation correction, to ensure consistent representation of facial features across different images.

2) Feature extraction: A convolutional neural network (CNN) is employed to extract high-dimensional feature vectors from the facial images, as shown in Figure 3[16]. DeepFace employs multiple convolutional and fully connected layers to learn both local and global features of the images.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

3) Feature comparison: Face matching is performed by computing the similarity between the feature vectors of two facial images. DeepFace utilizes cosine similarity to measure the resemblance between two vectors, with a similarity close to 1 indicating that the images belong to the same person.

DeepFace has been evaluated on public datasets such as Labeled Faces in the Wild (LFW), achieving impressive results. On the LFW dataset, DeepFace achieves an accuracy of over 97%, approaching human-level accuracy when compared with human judgments.

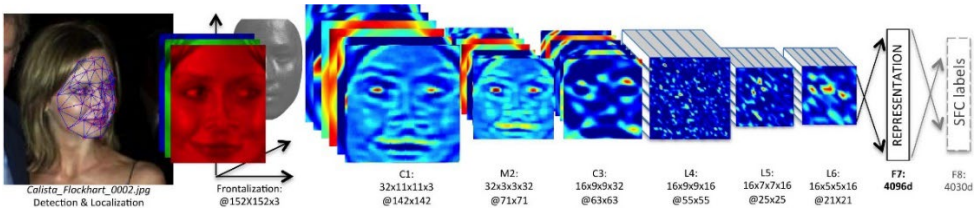

Figure 3: DeepFace extracts features with a multi-layer convolutional neural network.

Google's FaceNet[17], introduced in 2015, further pushed the boundaries by using a large amount of data and deep neural networks. FaceNet showed that it was not just capable of facial recognition, but also of clustering and verification, adding another layer of versatility to this technology. Its main objective is to learn a mapping of face images into a high-dimensional feature space where similar faces are clustered closely together. By learning embedding vectors of face images, FaceNet achieves accurate face recognition by ensuring that the distances between embeddings of the same person are small, while the distances between embeddings of different people are large.

The model architecture of FaceNet consists of a deep convolutional neural network (CNN), with the key component being the triplet loss function. This loss function aims to optimize the representation of embedding vectors by selecting appropriate triplet samples (anchor, positive, and negative). Specifically, the triplet loss function encourages the distance between embeddings of the anchor and positive samples to be as small as possible, while ensuring that the distance between embeddings of the anchor and negative samples is larger than a predefined negative distance threshold.

The training process involves the following steps:

1) Anchor: Select a face image as the anchor, whose embedding vector will be optimized.

2) Positive: Select another face image belonging to the same person as the anchor as the positive sample, aiming for a small distance between their embeddings.

3) Negative: Select a face image belonging to a different person as the negative sample, aiming for a large distance between their embeddings and the anchor's embedding.

By minimizing the triplet loss function, the goal is to reduce the distance between the anchor and positive samples while increasing the distance between the anchor and negative samples, as shown in Figure 4[17]. This encourages the embeddings of the same person to cluster together in the embedding space, while embeddings of different people are pushed apart.

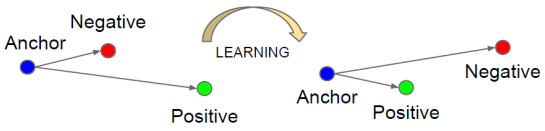

Figure 4: The Triplet Loss of FaceNet.

The FaceNet model architecture consists of multiple convolutional layers and fully connected layers to extract features from face images. Additionally, techniques such as batch normalization and Euclidean distance are employed to optimize the training process and representation of embedding vectors, as shown in Figure 5[17]. Through training on large-scale face image datasets, FaceNet can generate discriminative face embedding vectors, enabling efficient and accurate face recognition systems.

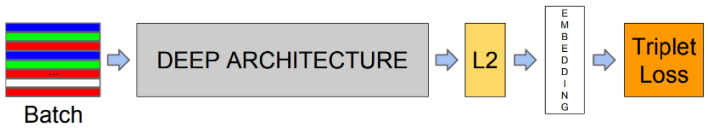

Figure 5: Model structure of FaceNet.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

Facial recognition has since become increasingly pervasive and integrated into our everyday lives. Whether unlocking our smartphones, tagging friends on social media, or crossing immigration at the airport, facial recognition technology is often at play, and continues to evolve.

The emergence of real-time facial recognition, which can identify individuals in live video feeds, has significant implications for security and surveillance. Meanwhile, developments in emotion recognition are opening up new possibilities for understanding human behavior and personalizing interactions.

In summary, the history and evolution of facial recognition technology has been characterized by continual advancements, each building on the last. From its initial stages of manual input and identification in the 1960s, to the integration of advanced machine learning and AI techniques in recent years, facial recognition technology has come a long way. Despite the impressive progress, the technology is still developing, with new research and advancements on the horizon promising even more sophisticated and versatile facial recognition systems.

3. Types of Facial Recognition Systems

Facial recognition technology has evolved significantly over the years, leading to the development of multiple systems with different techniques for capturing and analyzing facial data. Broadly, these systems can be classified into three categories: 2D Facial Recognition, 3D Facial Recognition, and Thermal Facial Recognition.

3.1. 2D Facial Recognition

2D facial recognition is the most common and widely used form of facial recognition technology[18]. It operates by capturing a two-dimensional image of a person's face and then comparing or verifying this image with stored 2D facial data. The most crucial factor in this type of system's success is the lighting conditions during the capture of the facial image. Changes in lighting can lead to changes in the appearance of facial features, which can potentially reduce accuracy.

2D facial recognition systems are also sensitive to the angle of the face[19]. They work best when the face is directly facing the camera, and performance tends to decrease when the face is turned to the side or tilted up or down. To mitigate this, advanced 2D facial recognition systems use AI techniques to estimate the appearance of the face from different angles.

Despite these challenges, 2D facial recognition systems have been widely adopted due to their relative simplicity and lower cost compared to other types. They are used extensively in various applications, including smartphone unlocking, photo tagging on social media, and security surveillance.

3.2. 3D Facial Recognition

3D facial recognition systems add another dimension to the process, capturing a three-dimensional model of a face. This technology maps the face's unique features – such as the curves of the eye socket, nose, and chin – which remain unaffected by lighting conditions or facial expressions[20].

3D facial recognition technology uses depth sensors or stereo cameras to capture the precise shape and contours of a face. The collected data is then used to identify or verify a person's identity. Since these systems use 3D data, they are less affected by changes in lighting or face angle[21], making them more accurate in various conditions compared to 2D systems.

However, 3D facial recognition systems are generally more complex and costly to implement. They also require more processing power to analyze the 3D facial data. Despite these challenges, they are becoming increasingly popular, particularly in high-security applications where a high level of accuracy is required.

3.3. Thermal Facial Recognition

Thermal facial recognition is a relatively new and less common type of facial recognition technology. It uses thermal cameras to capture the heat patterns that are emitted from the face[22]. These heat patterns, which are unique to each individual, can be detected in both light and dark environments, making this system highly effective regardless of lighting conditions.

Thermal facial recognition has shown potential in various applications, especially those that require

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

the detection of faces in poorly lit or nighttime conditions[23]. However, the technology is still in its early stages of development, and the cost of thermal cameras can be a limiting factor for widespread adoption.

In conclusion, each type of facial recognition system has its strengths and weaknesses, and the choice of system depends on the specific requirements of the application. The advancement of technology and research is likely to lead to improvements in these systems and possibly the development of new types that leverage other facial characteristics or technologies. The future of facial recognition technology is exciting, with boundless possibilities for innovation and application.

4. How Facial Recognition Works

The process of facial recognition involves a series of steps, ranging from data acquisition to the final stage of matching. While the specifics may vary between different types and models of facial recognition systems, the general process remains the same.

4.1. Data Acquisition

The first step in facial recognition is data acquisition or the collection of facial data. This is typically done using cameras that capture either 2D images, 3D images, or thermal images, depending on the type of system. The images can be taken from various sources such as video surveillance, smartphone cameras, or dedicated facial recognition devices.

4.2. Face Detection

Once an image is captured, the next step is to detect the presence of any faces in the image. This process involves identifying and locating human faces in digital images. Advanced algorithms are used to scan the entire image and distinguish facial features from the rest of the image based on certain properties or features such as the structure, color, and shape of the face.

4.3. Feature Extraction

After detecting a face in an image, the system then moves on to feature extraction. This process involves identifying and measuring distinct facial features and converting them into numerical data. The facial features that are commonly measured include the distance between the eyes, the width of the nose, the depth of the eye sockets, the shape of the cheekbones, and the length of the jawline, among others.

Different facial recognition systems extract and use different types of features. Some systems, like eigenface-based systems, look at the face as a whole and capture holistic features. Others, like local feature analysis systems, focus on specific local features like the eyes, nose, and mouth.

4.4. Matching

The final step in the facial recognition process is matching. This involves comparing the extracted features with the stored facial data in the database. In identification mode, the system compares the features with all the facial data in the database to find a match. In verification mode, the system compares the features with the stored data of a specific individual to confirm their identity.

In some systems, the match is determined based on a similarity score. If the similarity score crosses a certain threshold, the system concludes that it has found a match.

In recent years, machine learning, and more specifically deep learning, has been widely used in feature extraction and matching processes. Deep learning algorithms can learn to recognize patterns in the facial data, improving the accuracy and efficiency of the facial recognition process.

In summary, the overall process of facial recognition technology is shown in Figure 6, facial recognition involves a combination of sophisticated techniques and technologies. While the steps of data acquisition, face detection, feature extraction, and matching form the basis of all facial recognition systems, the specific implementation of each of these steps can vary widely, leading to different levels of performance and accuracy.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

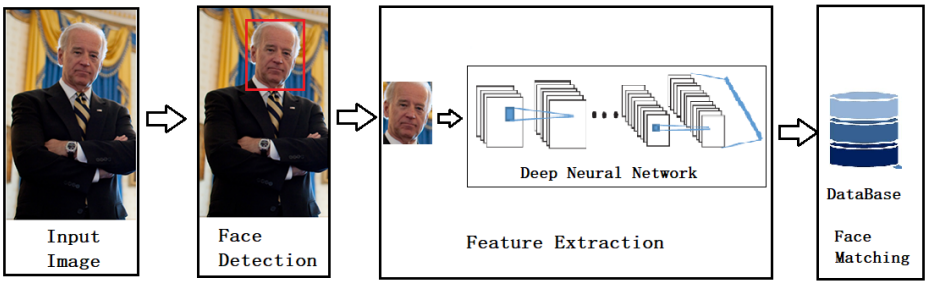

Figure 6: Facial recognition system process with deep learning model.

5. Applications of Facial Recognition Technology

Facial recognition technology has seen a surge in applications across a wide range of industries, driven by its potential to enhance security, convenience, and personalization.

5.1. Security and Surveillance

One of the most significant applications of facial recognition technology is in security and surveillance[24]. Law enforcement agencies across the globe use facial recognition to identify individuals in surveillance footage[25], helping to solve crimes and enhance public safety. The technology is also widely used in access control systems, providing secure entry to buildings or rooms by verifying the identity of individuals[26-28].

5.2. Smartphone Authentication

With the advent of smartphones equipped with advanced cameras and processing power, facial recognition has become a standard feature for device authentication[29-31]. Apple's Face ID[32], for example, uses a sophisticated 3D facial recognition system to unlock iPhones securely, providing a convenient alternative to passwords or PINs.

5.3. Social Media

Social media platforms like Facebook use facial recognition technology to automate the tagging of individuals in photos. By recognizing and remembering the facial data of users, these platforms can suggest tags for people in newly uploaded photos, enhancing the user experience and connectivity among users[33-37].

5.4. Healthcare

In the healthcare industry, facial recognition technology is being explored for various applications. Some systems use facial recognition to ensure patient identity and security. Research is also being conducted into recognizing certain diseases or health conditions that may affect facial features[38-43].

5.5. Retail

In the retail sector, facial recognition is used to enhance customer experience and security. Some stores use facial recognition to identify VIP customers as they enter, allowing staff to provide personalized service[44-47]. Facial recognition is also used to detect and deter shoplifting, contributing to loss prevention efforts[48-49].

These applications represent just a fraction of the potential uses of facial recognition technology. As the technology continues to advance, it is likely to be integrated into even more areas, including banking, travel, entertainment, and more. Despite the impressive benefits and applications, facial recognition technology also presents notable challenges, including accuracy concerns and issues related to privacy and ethics, which need to be carefully managed as the technology continues to evolve.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

6. Challenges and Limitations of Facial Recognition Technology

Despite its impressive capabilities and growing applications, facial recognition technology is not without its challenges and limitations.

6.1. Accuracy and Biases

Although facial recognition technology has significantly improved over time, there are still concerns about its accuracy. Changes in lighting[50], facial expressions[51], aging[52], and the use of accessories like glasses[53] or hats can sometimes affect the performance of facial recognition systems. Additionally, some facial recognition systems have been criticized for racial and gender biases[54], with lower accuracy rates observed for certain demographic groups. This has raised serious concerns about the fairness and reliability of the technology.

6.2. Privacy Concerns

The widespread use of facial recognition technology has also raised substantial privacy concerns[55]. The ability to identify and track individuals in public spaces could potentially lead to mass surveillance, infringing on people's privacy rights. There are also concerns about the storage and handling of sensitive facial data[56], which, if not properly protected, could be vulnerable to data breaches or misuse.

6.3. Regulatory and Legal Issues

Facial recognition technology is advancing at a much faster pace than the legal and regulatory frameworks that govern its use. Different countries have different laws and regulations related to facial recognition[57-60], and in some cases, the legal framework is lacking or unclear. This lack of consistent regulation can lead to misuse of the technology and can also create challenges for businesses operating in multiple jurisdictions.

6.4. Dependence on Quality of Input Data

The performance of facial recognition systems heavily depends on the quality of the input data. Low-resolution images or images captured at odd angles can lead to inaccurate results. This dependence on input quality can limit the effectiveness of facial recognition in certain scenarios[61-63].

Despite these challenges and limitations, the potential of facial recognition technology is immense. As the technology continues to evolve, it is likely that solutions to these challenges will be developed. Ongoing research and development, coupled with thoughtful regulation and ethical considerations, can help to ensure that the benefits of facial recognition technology are realized while minimizing potential drawbacks.

7. Future Prospects of Facial Recognition Technology

Facial recognition technology, despite the current challenges and limitations, is progressing at a rapid pace. Here are some prospective developments we might expect:

7.1. Improved accuracy

As the demand for facial recognition technology continues to grow, improving its accuracy remains a top priority. This involves refining algorithms to better handle variations in lighting, angles, facial expressions, and aging. Deep learning approaches, particularly those using convolutional neural networks (CNNs), have shown promise in this regard and are likely to be an area of continued research[64].

7.2. Bias correction

To tackle the bias issue, there's an increased focus on ensuring the diversity of training datasets[65]. In the future, we can expect more inclusive facial recognition systems that perform equally well across different genders, races, and age groups[66].

7.3. Privacy-preserving technologies

As privacy concerns become increasingly prominent, we might see the development of new methods

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

that allow for facial recognition without storing sensitive personal data. Techniques such as federated learning and differential privacy are being explored for this purpose[67].

7.4. Regulatory developments

In response to the growing use of facial recognition technology and associated issues, it's expected that more comprehensive regulations will be put in place. This will likely involve clearer guidelines for use and data handling practices[68].

7.5. Anti-spoofing techniques

To combat the issue of tricking facial recognition systems, advancements in liveness detection and anti-spoofing techniques are expected[69]. This could include algorithms that detect movement, depth, texture, and other signs of a live person.

7.6. Integration with other biometrics:

Facial recognition may increasingly be used in combination with other biometric systems, such as iris or fingerprint recognition, for enhanced security and accuracy[70].

7.7. Widespread usage in various sectors:

From security and surveillance to health and commerce, the usage of facial recognition technology is likely to expand across various sectors[71]. We may see more personalized experiences in retail, automatic patient identification in healthcare, and improved public safety measures.

7.8. Edge computing:

With the advancements in edge computing, facial recognition could be performed directly on local devices, reducing the need for data transmission and storage, and thereby enhancing privacy and speed[72].

In conclusion, the future of facial recognition technology is bright and promising. Continued advancements in accuracy, security, personalization, and healthcare applications, coupled with responsible development and ethical considerations, will shape the direction and potential of this technology. As society adapts to the evolving landscape, facial recognition technology has the potential to transform various industries and further integrate into our daily lives.

8. Conclusions

Facial recognition technology has come a long way since its early stages, and it continues to evolve at a rapid pace. This comprehensive overview has explored the history, types, working principles, applications, challenges, and future prospects of facial recognition technology.

We have seen how facial recognition has progressed from manual input to advanced algorithms powered by artificial intelligence and deep learning. The technology has found its place in various domains, including security and surveillance, smartphone authentication, social media, healthcare, and retail. Its ability to enhance security, convenience, and personalization has made it increasingly prevalent in our digital society.

However, facial recognition technology is not without its challenges. Accuracy concerns, biases, privacy issues, and regulatory frameworks pose significant considerations. The responsible and ethical development, deployment, and use of facial recognition technology are vital to address these challenges and build trust among users and the public.

Looking to the future, facial recognition technology holds immense potential. Advancements in accuracy, performance, security applications, personalization, healthcare integration, and cross-domain collaboration are anticipated. Responsible innovation, accompanied by clear regulations and guidelines, will be essential to ensure that the benefits of facial recognition technology are maximized while mitigating potential risks.

As facial recognition technology continues to evolve, it is crucial to engage in ongoing dialogue, research, and collaboration among stakeholders, including technology developers, policymakers, privacy advocates, and the general public. By working together, we can harness the full potential of facial recognition technology while upholding privacy, fairness, and ethical considerations.

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

In conclusion, facial recognition technology has emerged as a powerful tool with a wide range of applications. Its impact on security, convenience, and personalization is undeniable. With responsible development and thoughtful implementation, facial recognition technology has the potential to shape the future, making our lives more secure, efficient, and tailored to individual needs while ensuring that privacy and ethical considerations remain at the forefront.

Acknowledgements

Thanks for the research fund of Xianyang Science and Technology Bureau (No: 2020K02-64) and Shaanxi Provincial Department of Science and Technology(No: 2020NY-023) support this study.

References

[1] Kostka, G., Steinacker, L., & Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. Public Understanding of Science, 30(6), 671-690.
[2] Smith, A. (2019). More than half of US adults trust law enforcement to use facial recognition responsibly. Pew Research Center, 5.
[3] Kaplan, A. M., & Haenlein, M. (2012). Social media: back to the roots and back to the future. Journal of systems and information technology, 14(2), 101-104.
[4] Mohammed, M. N., Syamsudin, H., Al-Zubaidi, S., AKS, R. R., & Yusuf, E. (2020). Novel COVID-19 detection and diagnosis system using IOT based smart helmet. International Journal of Psychosocial Rehabilitation, 24(7), 2296-2303.
[5] Shankar, V., Kalyanam, K., Setia, P., Golmohammadi, A., Tirunillai, S., Douglass, T., ... & Waddoups, R. (2021). How technology is changing retail. Journal of Retailing, 97(1), 13-27.
[6] Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (2016). Face recognition for authentication on mobile devices. Image and Vision Computing, 55, 31-33.
[7] Ciftci, O., Choi, E. K. C., & Berezina, K. (2021). Let's face it: are customers ready for facial recognition technology at quick-service restaurants? International Journal of Hospitality Management, 95, 102941.
[8] Liu, Y. L., Yan, W., & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. Telecommunications Policy, 45(5), 102155.
[9] Van Noorden, R. (2020). The ethical questions that haunt facial-recognition research. Nature, 587(7834), 354-359.
[10] Dey, D. (2017). Growing importance of machine learning in compliance and regulatory reporting. European Journal of Multidisciplinary Studies, 2(7), 255-258.
[11] Bledsoe, W. W. (1966). Man-machine facial recognition. Panoramic Research Inc., Palo Alto, CA.
[12] Goldstein, A. J., Harmon, L. D., & Lesk, A. B. (1971). Identification of human faces. Proceedings of the IEEE, 59(5), 748-760.
[13] Sirovich, L., & Kirby, M. (1987). Low-dimensional procedure for the characterization of human faces. Josa a, 4(3), 519-524.
[14] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1), 71-86.
[15] Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on pattern analysis and machine intelligence, 19(7), 711-720.
[16] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).
[17] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).
[18] Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics, 9(8), 1188.
[19] Sengupta, S., Chen, J. C., Castillo, C., Patel, V. M., & Jacobs, D. W.. (2016). Frontal to profile face verification in the wild. 2016 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE.
[20] Zhou, S., Xiao, S. (2018). 3D face recognition: a survey. Hum. Cent. Comput. Inf. Sci. 8, 35.
[21] Luo, J., Hu, F., & Wang, R. (2019). 3D face recognition based on deep learning. In 2019 IEEE International Conference on Mechatronics and Automation (ICMA) (pp. 1576-1581). IEEE.
[22] Rajpurkar, O. M., Kamble, S. S., Nandagiri, J. P., & Bide, P. J. (2020). A Survey on Engagement and Emotion Analysis in Theatre using Thermal Imaging. 2020 4th International Conference on

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

Electronics, Communication and Aerospace Technology (ICECA).
[23] Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., ... & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. Journal of Law and the Biosciences, 7(1), lsaa038.
[24] Zhang, Y. , Shao, J. , Ouyang, D. , & Shen, H. T. . (2018). Person Re-identification Using Two-Stage Convolutional Neural Network. 2018 24th International Conference on Pattern Recognition (ICPR).
[25] Lu, C. , & Tang, X. . (2014). Surpassing human-level face verification performance on lfw with gaussianface. Computer Science.
[26] Bashbaghi, S. , Granger, E. , Sabourin, R. , & Parchami, M. . (2018). Deep Learning Architectures for Face Recognition in Video Surveillance. 10.48550/arXiv.1802.09990.
[27] Grgic, M. , Delac, K. , & Grgic, S. . (2011). Scface – surveillance cameras face database. Multimedia Tools & Applications, 51(3), 863-879.
[28] Heng, W. , Jiang, T. , & Gao, W. . (2018). How to assess the quality of compressed surveillance videos using face recognition. IEEE Transactions on Circuits and Systems for Video Technology, PP, 1-1.
[29] Ehatisham-ul-Haq, Muhammad, Azam, Muhammad, Awais, & Naeem, et al. (2018). Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. Journal of Network & Computer Applications.
[30] Wasnik, P. , Raja, K. B. , Raghavendra, R. , & Busch, C. . (2017). Assessing face image quality for smartphone based face recognition system. International Workshop on Biometrics & Forensics. IEEE.
[31] Mi, C. , Xu, R. , & Lin, C. T. . (2019). Real-time recognition of smartphone user behavior based on prophet algorithms.
[32] Bud, & Andrew. (2018). Facing the future: the impact of apple faceid. Biometric Technology Today, 2018(1), 5-7.
[33] Hebbale, S. G. , Mukherjee, A. , & Seal, A. . (2019). People Search on Social Media Platform Using Face Recognition. SoutheastCon 2019.
[34] Afra, S. , & Alhajj, R. . (2020). Early warning system: from face recognition by surveillance cameras to social media analysis to detecting suspicious people. Physica, A. Statistical mechanics and its applications, 540.
[35] Indrawan, P., Budiyatno, S., Ridho, N. M., & Sari, R. F. (2013). Face recognition for social media with mobile cloud computing. International Journal on Cloud Computing: Services and Architecture, 3(1), 23-35.
[36] Norval, A., & Prasopoulou, E. (2017). Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks. New media & society, 19(4), 637-654.
[37] Cherepanova, V., Goldblum, M., Foley, H., Duan, S., Dickerson, J., Taylor, G., & Goldstein, T. (2021). Lowkey: Leveraging adversarial attacks to protect social media users from facial recognition. arXiv preprint arXiv:2101.07922.
[38] Libby, C., & Ehrenfeld, J. (2021). Facial recognition technology in 2021: masks, bias, and the future of healthcare. Journal of Medical Systems, 45(4), 39.
[39] Shamova, U. (2020). Face recognition in healthcare: general overview. Язык в сфере профессиональной коммуникации.—Екатеринбург, 2020, 748-752.
[40] Sardar, A., Umer, S., Rout, R. K., Wang, S. H., & Tanveer, M. (2023). A secure face recognition for IoT-enabled healthcare system. ACM Transactions on Sensor Networks, 19(3), 1-23.
[41] Praveen, G. B., & Dakala, J. (2020, January). Face recognition: Challenges and issues in smart city/environments. In 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS) (pp. 791-793). IEEE.
[42] Masud, M., Muhammad, G., Alhumyani, H., Alshamrani, S. S., Cheikhrouhou, O., Ibrahim, S., & Hossain, M. S. (2020). Deep learning-based intelligent face recognition in IoT-cloud environment. Computer Communications, 152, 215-222.
[43] Alhussein, M. (2016). Automatic facial emotion recognition using weber local descriptor for e-Healthcare system. Cluster Computing, 19, 99-108.
[44] Wright, E. (2018). The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector. Fordham Intell. Prop. Media & Ent. LJ, 29, 611.
[45] Mansfield-Devine, S. (2013). Biometrics in retail. Biometric Technology Today, 2013(9), 5-8.
[46] Dijmărescu, I., Iatagan, M., Hurloiu, I., Geamănu, M., Rusescu, C., & Dijmărescu, A. (2022). Neuromanagement decision making in facial recognition biometric authentication as a mobile payment technology in retail, restaurant, and hotel business models. Oeconomia Copernicana, 13(1), 225-250.
[47] Gao, J., Rong, Y., Tian, X., & Yao, Y. (2023). Improving Convenience or Saving Face? An Empirical Analysis of the Use of Facial Recognition Payment Technology in Retail. Information Systems Research.
[48] Martínez-Mascorro, G. A., Abreu-Pederzini, J. R., Ortiz-Bayliss, J. C., & Terashima-Marín, H. (2020). Suspicious behavior detection on shoplifting cases for crime prevention by using 3D

ISSN 2616-5775 Vol. 6, Issue 7: 15-26, DOI: 10.25236/AJCIS.2023.060703

convolutional neural networks. arXiv preprint arXiv:2005.02142.
[49] Martínez-Mascorro, G. A., Abreu-Pederzini, J. R., Ortiz-Bayliss, J. C., Garcia-Collantes, A., & Terashima-Marín, H. (2021). Criminal intention detection at early stages of shoplifting cases by using 3D convolutional neural networks. Computation, 9(2), 24.
[50] Adini, Y. , & Moses, Y. . (1997). Face recognition: the problem of compensating for changes in illumination direction. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), P.721-732.
[51] Nomi, J. S., Rhodes, M. G., & Cleary, A. M. (2013). Emotional facial expressions differentially influence predictions and performance for face recognition. Cognition & emotion, 27(1), 141-149.
[52] Chen, B. C., Chen, C. S., & Hsu, W. H. (2014). Cross-age reference coding for age-invariant face recognition and retrieval. In Computer Vision–ECCV 2014: 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part VI 13 (pp. 768-783). Springer International Publishing.
[53] Park, J. S., Oh, Y. H., Ahn, S. C., & Lee, S. W. (2005). Glasses removal from facial image using recursive error compensation. IEEE transactions on pattern analysis and machine intelligence, 27(5), 805-811.
[54] Herlitz, A., & Lovén, J. (2013). Sex differences and the own-gender bias in face recognition: A meta-analytic review. Visual Cognition, 21(9-10), 1306-1336.
[55] Bowyer, K. W. (2004). Face recognition technology: security versus privacy. IEEE Technology and society magazine, 23(1), 9-19.
[56] Senior, A. W., & Pankanti, S. (2011). Privacy protection and face recognition. Handbook of face recognition, 671-691.
[57] Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics, 2(3), 377-387.
[58] Eneman, M., Ljungberg, J., Raviola, E., & Rolandsson, B. (2022). The sensitive nature of facial recognition: Tensions between the Swedish police and regulatory authorities. Information Polity, (Preprint), 1-14.
[59] Wright, E. (2018). The future of facial recognition is not fully known: Developing privacy and security regulatory mechanisms for facial recognition in the retail sector. Fordham Intell. Prop. Media & Ent. LJ, 29, 611.
[60] Selinger, E., & Hartzog, W. (2020). The inconsentability of facial surveillance. Loy. L. Rev., 66, 33.
[61] Hu, Z., Gui, P., Feng, Z., Zhao, Q., Fu, K., Liu, F., & Liu, Z. (2019). Boosting depth-based face recognition from a quality perspective. Sensors, 19(19), 4124.
[62] Hernandez-Ortega, J., Galbally, J., Fiérrez, J., & Beslay, L. (2020). Biometric quality: Review and application to face recognition with faceqnet. arXiv preprint arXiv:2006.03298.
[63] Nech, A., & Kemelmacher-Shlizerman, I. (2017). Level playing field for million scale face recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 7044-7053).
[64] Ranjan, R., Sankaranarayanan, S., Bansal, A., Bodla, N., Chen, J. C., Patel, V. M., ... & Chellappa, R. (2018). Deep learning for understanding faces: Machines may be just as good, or better, than humans. IEEE Signal Processing Magazine, 35(1), 66-83.
[65] Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency (pp. 77-91). PMLR.
[66] De-Arteaga, M., Romanov, A., Wallach, H., Chayes, J., Borgs, C., Chouldechova, A., ... & Kalai, A. T. (2019, January). Bias in bios: A case study of semantic representation bias in a high-stakes setting. In proceedings of the Conference on Fairness, Accountability, and Transparency (pp. 120-128).
[67] Shokri, R., & Shmatikov, V. (2015, October). Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (pp. 1310-1321).
[68] Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology.
[69] Bousa, M., Anagnostopoulos, G., del Corro, E., Drogowska, K., Pekarek, J., Kavan, L., ... & Frank, O. (2016). Stress and charge transfer in uniaxially strained CVD graphene. physica status solidi (b), 253(12), 2355-2361.
[70] Jain, A. K., Ross, A. A., Nandakumar, K., Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Face recognition (pp. 97-139). Springer US.
[71] Grother, P. J., Grother, P. J., Ngan, M., & Hanaoka, K. (2014). Face recognition vendor test (FRVT). US Department of Commerce, National Institute of Standards and Technology.
[72] Liu, S., Liu, L., Tang, J., Yu, B., Wang, Y., & Shi, W. (2019). Edge computing for autonomous driving: Opportunities and challenges. Proceedings of the IEEE, 107(8), 1697-1716.