Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/87/20241560

Facial recognition - A literature review

Shengdi Wang

University of Sheffield, Sheffield S10 2TN, United Kingdom

shengdi777@gmail.com

Abstract. This paper analyses the main technologies for face recognition, a critical biometric tool for identity verification and security across various sectors. A comprehensive overview of traditional and modern facial recognition technologies will be provided, examining their key features such as age, pose, and illumination. The study discusses the evolution and current state of facial recognition, highlighting significant advancements and applications in recent years. The objective is to offer a detailed understanding of how these technologies function and their implications for security and identity verification.

Keywords: face recognition, biometrics, neural networks, applications.

1. Introduction

In recent years, facial recognition technology has significantly advanced[1], becoming an integral part of numerous security and identification systems around the world. Utilised for a variety of applications ranging from law enforcement to personal device security, this technology leverages unique facial features to identify or verify individuals. As a non-intrusive and user-friendly biometric solution, it is favoured in many public and private sectors. The reason why facial recognition technology can develop so rapidly is that it combines many factors: advanced active development of algorithms[5], the availability of a large database of facial images and plenty of methods for evaluating the performance of face recognition algorithms. However, facial recognition technology is facing significant challenges, including variable environmental conditions, ethical concerns, and the need for improved accuracy and privacy safeguards.

Biometric identification consists of determining the identity of a person. Biometrics can be divided into two types – behavioural and physiological.[3]The swift advancement of mobile technology has enabled the incorporation of biometric sensors into smart devices.[4]Physiological biometrics are based on unique physical characteristics which vary from individual to individual, such as fingerprints, iris patterns, facial features and hand geometry. Behavioural biometrics focus on unique patterns in personal activities and behaviours including voice, signature, odour and keystroke dynamics. Although the study of some physiological and behavioural biometrics like ear and nose structure or keystroke dynamics is still in early development stages, each biometric method offers distinct advantages and drawbacks. For example, although iris recognition has high accuracy, it is not cost-effective. Also fingerprints are easily collected but might not work well with uncooperative subjects.

In the realm of security and personal identification, biometrics is used to identify individuals based on their physiological or behavioural characteristics. These methods have been foundational in various applications ranging from secure access control systems to personal device security and law enforcement.

DOI: 10.54254/2755-2721/87/20241560

As technology is advancing, biometric systems have increasingly integrated into daily life, enhancing security protocols but also raising important privacy and ethical considerations. The choice of biometric technique which ranges from facial recognition to fingerprint scanning depends on the specific needs of the application, the required level of security, cost considerations and the acceptability of the technology to users. There are several aspects of the development of facial recognition.

Face recognition algorithms fall into two categories: fully automatic and partially automatic. Fully automatic algorithms handle the entire process independently, from detecting and normalising the face to identifying the individual by comparing features against a database. Partially automatic algorithms need additional data, such as the coordinates of key facial landmarks, to aid in normalisation and identification. The choice between these algorithms depends on automation needs, accuracy, and available computational resources.

Face recognition technology is also classified based on image orientation into frontal, profile, and view-tolerant recognition. Frontal recognition requires direct camera facing and is used in controlled environments like access control systems. Profile recognition handles side views and is suitable for surveillance where direct facing is not possible. View-tolerant recognition can identify faces from various angles, making it ideal for dynamic environments like crowded public spaces. These types enhance biometric systems' versatility, catering to applications from secure access to public safety monitoring.

- Pose

The variability in a person's pose—whether they are facing forward, looking to the side, or tilting their head—poses a substantial challenge for facial recognition systems[2]. A change in head position can alter the appearance of facial features in ways that are not always predictable, making consistent recognition difficult. This issue has been a focal point in facial recognition research for decades. Advances in 3D modelling and multi-angle recognition have been developed to address these challenges. Techniques like view-tolerant recognition algorithms are designed to handle images captured from various angles, but there is still considerable work to be done to perfect these methods across all potential use cases.

- Illumination

Lighting conditions play a critical role in the performance of facial recognition systems[3]. Variations in lighting can create shadows, highlight certain facial features, or obscure others, leading to inconsistent inputs for recognition algorithms. This variability can significantly degrade the accuracy of facial recognition. Researchers are actively exploring solutions to make facial recognition systems more robust against changes in lighting. Techniques such as using infrared illumination or developing algorithms that can normalise lighting conditions in images are among the approaches being considered to mitigate the effects of variable lighting.

- Age

As people age, facial features change significantly, posing challenges for facial recognition systems. Research is ongoing to develop dynamic algorithms and machine learning models that adapt to these changes over time.

Despite advances, two major limitations remain. Firstly, no system can fully handle all facial variations like pose, illumination, expression, and age. Secondly, these systems perform better with more training images, but obtaining extensive datasets is often limited by privacy, logistics, or rare conditions, impacting their effectiveness in diverse environments.

DOI: 10.54254/2755-2721/87/20241560

2. Traditional facial recognition technologies

2.1. Eigenface

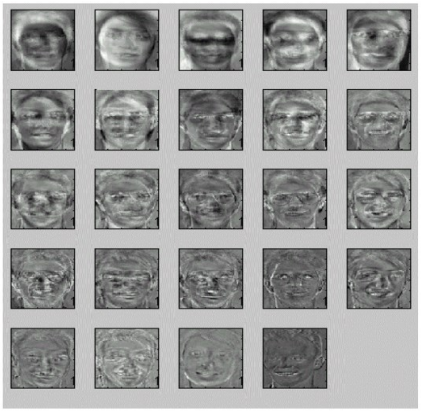

Figure 1. Eigenfaces for sample faces[8]

Eigenface, a key method in facial recognition, relies on Principal Component Analysis (PCA) to reduce image complexity and transform faces into eigenfaces, capturing main variations in features. Each face is represented as a weighted combination of these eigenfaces, with recognition achieved by comparing feature vectors derived from them.

Eigenface is efficient, compressing data significantly and allowing rapid processing during training. It has achieved varied accuracy, with a database of 2,500 images showing correct classifications at rates of 96%, 85%, and 64% for lighting, orientation, and size variations, respectively. However, it requires consistent image quality and conditions, performing poorly with significant variations in lighting, pose, and scale. Faces must be aligned similarly for effective recognition.

The method also struggles with ageing and facial expressions. Adaptations like eigenfeatures target specific components (e.g., eyes, nose) to improve sensitivity to appearance changes. Combining face recognition with other biometrics, such as ear measurements, has significantly improved recognition rates; for example, combining ear and face data increased the rate from 70.5% to 90.9%.

In summary, eigenface is suitable for controlled environments where conditions are standardised, offering a fast and straightforward technique, ideal when speed and simplicity are prioritised over high precision.

2.2. Neural networks

Neural networks have significantly advanced the field of facial recognition by leveraging their inherent non-linearity[9], which enhances the efficiency of the feature extraction process beyond what linear methods like the Karhunen-Loève can achieve. One of the earliest applications of artificial neural networks (ANNs) in facial recognition involved the use of a single-layer adaptive network called WIZARD, which set the foundation for more complex systems like multilayer perceptrons and convolutional neural networks (CNNs). These networks handle tasks from basic face detection to more complex face verification with high accuracy, often incorporating innovative structures such as multi-resolution pyramids and hybrid systems that combine local image sampling with self-organising maps.

A critical advantage of neural networks is their ability to adapt to the variability in facial images through structures that allow for the dimensional reduction of data and partial invariance to changes in translation, rotation, scale, and deformation. For example, hybrid networks reported recognition accuracies as high as 96.2% on databases like the ORL, with 400 images of 40 individuals. However, neural networks are not without challenges; they require extensive training times, with some models taking up to four hours to train, though classification can be completed in under half a second.

DOI: 10.54254/2755-2721/87/20241560

2.3. Graph matching

Graph matching is a sophisticated approach in face recognition, using dynamic link structures and elastic graph matching to handle variations in orientation and expression. Each face is represented by a graph with nodes at specific facial landmarks and edges capturing geometric distances. Features like Gabor filter responses characterise each node.

Elastic Bunch Graph Matching (EBGM) is a notable implementation, organising graphs into a face bunch graph for efficient comparisons. This method handles nonlinear variations such as illumination, pose, and expression, achieving recognition rates up to 98%. It demonstrated high rotation invariance, with success rates of 86.5% and 66.4% for 15 and 30-degree rotations, respectively.

However, graph matching is computationally intensive; comparing 87 objects took about 25 seconds on a system with 23 transputers. It also requires high-resolution images to accurately localise landmarks, posing challenges in scenarios like surveillance with distant or lower-resolution captures. Despite these challenges, graph matching is powerful for managing precise rotational and expressive variability in face recognition.

2.4. 3D morphable model

Figure 2. Different light directions have influence on 3D model fitting[4]

The 3D morphable model in facial recognition uses a vector space representation of faces, combining shape and texture vectors to depict human faces realistically. By fitting these 3D models to images, the system operates under two paradigms: using model coefficients to capture intrinsic face features and creating synthetic views for viewpoint-dependent recognition.

This method incorporates deformable 3D models and computer graphics to estimate 3D shape, texture, and scene parameters like illumination and projection from a single image. It handles non-Lambertian reflections, specular reflections, and cast shadows, automatically adjusting for head position, camera focal length, and illumination. An initialization procedure using six to eight facial points enhances model setup.

Empirical results show the model's efficacy, with 95% accuracy on the CMU-PIE database using side-view galleries and 95.9% on the FERET set with frontal views. Despite requiring high-quality 3D scans and being computationally intensive, the 3D morphable model offers high-precision recognition across diverse conditions, marking a significant advancement in facial recognition.

DOI: 10.54254/2755-2721/87/20241560

3. Modern facial recognition technologies

3.1. Line Edge Map(LEM)

Figure 3. An illustration of a face LEM[12]

The Line Edge Map (LEM) approach in facial recognition leverages edge information, which is less sensitive to illumination variations. LEM uses edge maps to capture facial feature boundaries, maintaining consistent visibility despite lighting changes. By converting edge maps into line segments through polygonal line fitting, LEM reduces model complexity, storing only segment endpoints for a simplified face representation.

The process involves thinning the edge map for precise line fitting, creating an efficient data structure. LEM has shown superior performance, achieving perfect or near-perfect identification rates of 100% and 96.43% on specific databases. It matches the eigenface method's performance under ideal conditions and excels in handling slight appearance and size variations.

However, LEM is sensitive to pose and significant facial expression changes, making it less effective in dynamic environments. Despite this, LEM is a robust, storage-efficient solution for facial recognition, particularly suitable for applications with variable lighting where edge detail is crucial for identity verification.

Table 1. Performance Comparison on the AR Database [11]

Method	Recognition rate
LEM	96.43%
Eigenface (20-eigenvectors)	55.36%
Eigenface (60-eigenvectors)	71.43%
Eigenface (112-eigenvectors)	78.57%

According to the table, it can be found that the recognition rate of LEM is the best, compared to other methods.

3.2. Support Vector Machine(SVM)

Support Vector Machines (SVM) are highly effective for face recognition, leveraging an Optimal Separating Hyperplane (OSH) to maximise the margin between classes, minimising misclassification risk. This is achieved through Structural Risk Minimization (SRM), optimising both training and generalisation errors, making SVM suitable for limited training samples.

SVMs handle high-dimensional data well, ideal for face recognition with numerous input features. Kernels allow SVMs to operate in transformed feature spaces, managing complex, nonlinear relationships. This enables effective modelling of facial image similarities and dissimilarities for verification and identification tasks.

DOI: 10.54254/2755-2721/87/20241560

Challenges include computational intensity, particularly with large datasets and complex Quadratic Programming (QP) during training. Decomposition algorithms help mitigate this, but performance can degrade with many classes (individual faces).

Empirical results highlight SVM robustness in face recognition, achieving 92% accuracy with edge maps and outperforming traditional methods like eigenfaces under varying conditions. For example, SVMs achieved an 8.79% error rate compared to 15.14% with Nearest Center Classification (NCC) using eigenfaces. SVMs also excel in multi-view face detection, with over 90% recognition accuracy and a 95% detection rate in video sequences.

Overall, SVMs offer high accuracy and robustness in face recognition, despite some computational and scalability challenges.

3.3. Multiple Classifier Systems(MCSs)

Multiple Classifier Systems (MCSs) enhance face recognition by integrating outputs from various classifiers, improving accuracy and robustness. This approach leverages the diverse strengths of classifiers like Learning Vector Quantization (LVQ), Radial Basis Function (RBF) neural networks, Eigenfaces, Fisherfaces, Support Vector Machines (SVM), and Elastic Graph Matching (EGM). By combining different classifiers, MCSs reduce uniform errors and handle variations in pose, expression, and illumination better than single classifiers.

Hybrid methods using both holistic and feature-based analyses, like the Markov Random Field (MRF) model, also performed well, with recognition rates of 96.11% on Yale and 86.95% onORL.

Designing and training MCSs can be complex and computationally expensive due to the need to integrate multiple classifiers effectively. However, their superior accuracy and adaptability to varied data conditions make MCSs a powerful tool in advanced face recognition systems.

4. Application

- Security access control

Facial recognition technology is increasingly used in high-security access control systems, such as the Chui doorbell by Trueface.ai, which employs deep learning to distinguish real faces from photos, preventing fraud. This system scans a face and compares it to a database of authorised individuals, granting access if a match is found. While enhancing security and convenience by eliminating the need for physical keys, it raises privacy concerns over sensitive biometric data and can be affected by poor lighting or changes in appearance. Despite these issues, facial recognition remains a valuable tool for secure access control.

- Surveillance systems

Surveillance systems, especially those using facial recognition technology, are increasingly deployed across various sectors for enhanced security and monitoring. These systems utilise CCTV cameras installed at strategic locations to capture video footage, which is then processed to identify individuals based on facial recognition.

The principle behind these systems involves capturing live video feeds, extracting faces, and matching them against a database of known individuals to identify potential offenders or track customer behaviour.

However, while facial recognition in surveillance offers considerable benefits such as enhanced security and loss prevention, it also comes with drawbacks. Privacy concerns are significant, as there is the potential for misuse of personal biometric data. Furthermore, the accuracy of these systems can be affected by various factors including poor lighting, obstructions, or changes in appearance. Despite these challenges, facial recognition remains a powerful tool in modern surveillance systems, providing a mix of proactive security and substantial utility in public safety operations.

- General identity verification

DOI: 10.54254/2755-2721/87/20241560

General identity verification systems increasingly incorporate facial recognition technology to validate personal identities using important documents such as national identification cards and passports. The core principle involves capturing a facial image of the individual, which is then digitised and stored as part of their official identity record. During verification, the stored image is compared with a live capture or another submitted image to confirm the person's identity.

This method provides a quick and efficient way of confirming identities, enhancing security for various administrative and legal processes. However, it also raises privacy concerns due to the storage and handling of personal biometric data. Additionally, the accuracy of facial recognition can be compromised by poor image quality or changes in a person's appearance over time. Despite these potential drawbacks, facial recognition in identity verification remains a valuable tool for enhancing security and streamlining identification processes.

5. Conclusion

Facial recognition technology is widely used in security, surveillance, and personal device access. It strengthens access control by verifying identities through deep learning algorithms, and in surveillance, it helps monitor and identify individuals in places like banks and malls, reducing criminal activities. For identity verification, it's used in passports and national IDs, matching individuals with biometric data in government databases. On personal devices, facial recognition offers a quick alternative to PINs and passwords, despite challenges with environmental variations and security vulnerabilities.

However, this technology raises privacy concerns due to the risks of data breaches and unauthorised surveillance. Its effectiveness can also be affected by poor lighting, changes in appearance, and capture angles. Despite these issues, facial recognition continues to evolve, enhancing security and user experience in various applications.

References

[1] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM computing surveys (CSUR)*, *35*(4), 399-458.

[2] Adini, Y., Moses, Y., & Ullman, S. (1997). Face recognition: The problem of compensating for changes in illumination direction. *IEEE Transactions on pattern analysis and machine intelligence*, *19*(7), 721-732.

[3] Jain, A. K., & Li, S. Z. (2011). *Handbook of face recognition* (Vol. 1, p. 699). New York: springer.

[4] Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, *60*(2), 131-139.

[5] Zhou, S. K., & Chellappa, R. (2005). Image-based face recognition under illumination and pose variations. *JOSA A*, *22*(2), 217-229.

[6] Partridge, D., & Griffith, N. (2002). Multiple classifier systems: Software engineered, automatically modular leading to a taxonomic overview. *Pattern Analysis & Applications*, *5*, 180-188.

[7] Lanitis, A., Taylor, C. J., & Cootes, T. F. (2002). Toward automatic simulation of ageing effects on face images. *IEEE Transactions on pattern Analysis and machine Intelligence*, *24*(4), 442-455.

[8] Ellavarason, E., Guest, R., Deravi, F., Sanchez-Riello, R., & Corsetti, B. (2020). Touch-dynamics based behavioural biometrics on mobile devices–a review from a usability and performance perspective. *ACM Computing Surveys (CSUR)*, *53*(6), 1-36.

[9] Kshirsagar, V. P., Baviskar, M. R., & Gaikwad, M. E. (2011, March). Face recognition using Eigenfaces. In *2011 3rd International Conference on Computer Research and Development* (Vol. 2, pp. 302-306). IEEE.

[10] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of cognitive neuroscience*, *3*(1), 71-86.

[11] Gao, Y., & Leung, M.K. (2002). Face Recognition Using Line Edge Map. *IEEE Trans. Pattern Anal. Mach. Intell., 24*, 764-779.

DOI: 10.54254/2755-2721/87/20241560

[12] Yongsheng Gao and M. K. H. Leung, "Face recognition using line edge map," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 6, pp. 764-779, June 2002.

[13] 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).

[14] Ratcliffe, J. (2006). *Video surveillance of public places*. Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.