World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Exploring integrated biometric surveillance systems: Case studies and future trends

Varinder Kaur Attri [1], Teena Jaiswal [2,*], Ram Narayan Jaiswal [3] and Vidhu Baggan [4]

[1] *Department of CSE, GNDU, RC Jalandhar, India.*
[2] *Department of CS, GNDU, Amritsar, Punjab, India.*
[3] *Bundelkhand University Jhansi, India.*
[4] *Department of CSE, Chitkara University, Himachal Pradesh, India.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 14(02), 208-215

Publication history: Received on 05 January 2025; revised on 13 February 2025; accepted on 16 February 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.14.2.0073

Abstract

Biometric systems have become integral to modern security protocols due to their high accuracy and reliability. Integrated surveillance systems combine various biometric methods with advanced monitoring technology to enhance security and facilitate real-time tracking. This paper explores several case studies that demonstrate the application of integrated surveillance systems, particularly in the context of biometric technologies such as facial recognition, fingerprint scanning, iris recognition, and voice recognition. The research examines how these systems are implemented across different industries, their benefits, challenges, ethical consideration and potential for future developments.

Keywords: Integrated Surveillance Systems; Biometric Technologies; Real-Time Tracking; Facial Recognition

1. Introduction

The rapid growth of technology in recent years has resulted in the development of more sophisticated surveillance systems. The need for heightened security in both public and private sectors has driven the demand for integrated surveillance systems. A key component of these systems is biometric authentication, which uses unique physiological or behavioral characteristics to identify individuals. Biometric systems are highly efficient, providing more accuracy and security than traditional methods like passwords or PIN codes [34]. Signature verification stands as a vital element of biometric recognition, playing an indispensable role in ensuring security and authenticity in forensic investigations, legal documents, and financial transactions. Its importance cannot be overstated [37]. This paper discusses case studies of integrated surveillance systems that leverage biometric technologies. It also explores the potential applications, implications, ethical consideration and challenges of combining biometric authentication with surveillance systems to create more secure environments.

1.1. Background of Biometric Surveillance Systems

Biometric surveillance systems combine the capabilities of biometric authentication technologies with surveillance equipment to monitor and identify individuals. These systems often employ multi-modal biometrics, which combine two or more biometric traits (e.g., facial and fingerprint recognition) to improve accuracy and reduce errors.

* Corresponding author: Teena Jaiswal.

1.2. Biometric Technologies:

- **Facial Recognition**: An advanced method of identifying or verifying individuals based on their facial features. Facial recognition has been increasingly adopted in surveillance systems because of its non-intrusive nature and the ability to capture individuals from a distance. Facial Recognition: Utilizes algorithms to identify individuals based on facial features, increasingly integrated with AI for improved accuracy [1].
- **Fingerprint Recognition**: One of the most widely used biometric methods, fingerprint scanning offers high precision and reliability for identification purposes. It is used in various applications, including access control in secure areas. Fingerprint Scanning: A widely used method that maps unique patterns in fingerprints, often enhanced by machine learning techniques[1].
- **Iris Recognition**: Iris scanning analyzes the unique patterns in the human iris to identify individuals. Due to its high accuracy, it is often used in high-security areas where other methods may be insufficient. Iris Recognition: Offers high accuracy due to the uniqueness of iris patterns, making it suitable for secure applications [2].
- **Voice Recognition**: This technology analyzes vocal patterns and speech characteristics for identification. It has been integrated into several surveillance systems to complement other biometric methods. Voice Recognition: Analyzes vocal characteristics for authentication, though it faces challenges from spoofing attacks[3].

The integration of biometric systems into surveillance allows for seamless monitoring of individuals in real-time, especially in high-security environments such as airports, government buildings, and private enterprises. The systems can be linked to a central database for automated verification, alerting security personnel to unauthorized access or suspicious activity. This paper examines integrated surveillance systems with a focus on real-world implementations, providing insights into both the benefits and challenges of using biometric systems.

2. Literature Review

Biometric technologies, including facial recognition, fingerprint scanning, iris recognition, and voice recognition, have transformed identity verification and security systems. These technologies leverage unique biological traits to enhance accuracy and user experience while addressing various challenges such as privacy concerns and security vulnerabilities. Combines multiple biometric traits (e.g., fingerprints and facial recognition) to enhance security and reduce false acceptance rates[4]. Eliminates the need for passwords, providing a seamless user experience[4]. Despite the advancements in biometric technologies, concerns regarding privacy and data security persist. The potential for misuse of biometric data and the ethical implications of surveillance technologies necessitate ongoing research and regulatory frameworks to protect individual rights[2][5]. Facial recognition technology offers numerous advantages in security systems, enhancing both efficiency and effectiveness in various applications. Its ability to provide real-time identification and monitoring significantly improves security measures across different environments, from residential to industrial settings. the primary benefits of implementing facial recognition technology in security systems are

2.1. Enhanced Security and Access Control

Automated Unlocking: Systems utilizing facial recognition can unlock doors automatically, reducing reliance on traditional locks that are vulnerable to tampering [6].Integration with CCTV allows for continuous surveillance, enabling immediate identification of unauthorized individuals[7]. Facial recognition can identify repeat offenders, aiding law enforcement in crime prevention efforts. Reports indicate that a significant percentage of crimes are committed by the same individuals. The technology can assist in locating missing individuals by analyzing footage from public spaces[8].

2.2. Efficiency and Privacy

Automated systems minimize the need for constant human monitoring, enhancing operational efficiency [7].Advanced techniques, such as homomorphic encryption, ensure that personal data remains confidential during recognition processes[9].While facial recognition technology presents significant advantages, concerns regarding privacy and potential misuse remain prevalent. Balancing security benefits with ethical considerations is crucial for its responsible implementation. Fingerprint scanning technology significantly enhances user experience in identity verification by providing a combination of security, usability, and efficiency. This technology leverages unique biometric data, ensuring a reliable and user-friendly authentication process.

2.3. Enhanced Security

Fingerprint scanning offers a higher level of security compared to traditional methods like passwords, as it relies on unique biological [10]. Systems that combine fingerprint verification with additional security measures, such as passwords, further mitigate risks associated with data theft [11].

2.4. Usability and User Experience

Studies show that systems like the Mobile Automated Fingerprint Identification System (MAFIS) achieve high usability scores, indicating that users find them easy to use and efficient [12]. The User Experience Questionnaire (UEQ) highlights dimensions such as attractiveness and dependability, which contribute to positive user interactions with fingerprint systems [12].

2.5. Practical Applications

Fingerprint technology is widely adopted in various sectors, including mobile devices, border control, and secure access, demonstrating its versatility and effectiveness in real-world applications [10].

While fingerprint scanning technology offers numerous advantages, concerns regarding the permanence and uniqueness of fingerprints remain, suggesting that further research is needed to address these challenges and enhance the reliability of biometric systems [10].

2.6. Ethical considerations

The use of biometric technologies in surveillance raises significant ethical considerations, primarily concerning privacy, consent, and the potential for misuse. As these technologies become more integrated into security frameworks, it is crucial to address the implications they have on individual rights and societal norms.

2.7. Privacy Concerns

Biometric data, such as facial recognition and fingerprints, can lead to unauthorized surveillance and data breaches, compromising individual privacy [13][14]. The collection and storage of biometric information pose risks of identity theft and misuse, necessitating stringent data protection measures [14].

2.8. Consent and Autonomy

The ethical application of biometric technologies requires informed consent from individuals, which is often overlooked in mass surveillance contexts [15]. Individuals may not fully understand how their biometric data will be used, leading to a violation of personal autonomy [16].

2.9. Societal Implications

The deployment of biometric surveillance can perpetuate social biases, particularly against marginalized groups, as seen in the policing of migration [17]. Ethical governance frameworks are essential to ensure that biometric technologies are used responsibly and do not reinforce systemic inequalities [17].

Conversely, proponents argue that biometric technologies can enhance security and efficiency in law enforcement, potentially reducing crime rates. However, this perspective often underestimates the long-term consequences of eroding privacy and civil liberties.

3. Case Studies of Integrated Biometric Surveillance Systems:

In this section, we examine several case studies where biometric systems have been integrated into surveillance infrastructure, demonstrating their effectiveness in real-world applications.

3.1. Case Study 1: Airport Security Systems – Facial and Fingerprint Recognition

At major international airports, biometric systems are widely used to improve security and streamline passenger flow [35]. For instance, Dubai International Airport has implemented an integrated biometric surveillance system that combines facial recognition and fingerprint scanning to enhance security during passenger check-ins and boarding.

- **Implementation**: The system employs facial recognition to match passengers with their passport photos upon arrival. Fingerprint scans are used as a secondary verification method for high-security areas. The system integrates with the airport's central security database to detect any individuals on watchlists.
- **Benefits**: Increased efficiency, reduced wait times, and enhanced security, particularly for identifying potential threats or individuals using fraudulent identification.
- **Challenges**: Privacy concerns, high cost of implementation, and the need for continuous updates to maintain system accuracy.

3.2. Case Study 2: Government Buildings – Iris and Voice Recognition

A government building in the United States has implemented an integrated biometric surveillance system using iris recognition and voice recognition for restricted areas[21]. The system provides dual authentication for employees and visitors, ensuring that access is granted only to authorized individuals.

- **Implementation**: The system integrates iris scanning terminals and voice recognition software at entry points. The iris scan provides a highly accurate verification method, while voice recognition is used for remote access to sensitive information via secure phone lines.
- **Benefits**: Improved security through multi-factor authentication and seamless integration with existing security systems. The dual-factor approach reduces the risk of identity fraud.
- **Challenges**: Environmental factors affecting iris scanning, such as poor lighting, and the risk of spoofing in voice recognition systems.

3.3. Case Study 3: Retail and Banking Sectors – Multi-Modal Biometric Integration

In the retail and banking sectors, the integration of biometric systems with surveillance cameras and point-of-sale systems is becoming more common. Retail stores have implemented multi-modal biometric systems to track individuals' behaviors, verify identities for credit card purchases, and reduce fraud.

- **Implementation**: Customers are identified via facial recognition and fingerprint scanning at checkout points. Surveillance cameras monitor movements, and transaction data is cross-referenced with biometric profiles to prevent fraudulent activity.
- **Benefits**: Reduction in credit card fraud, improved customer experience, and enhanced employee productivity. Integration with surveillance systems allows for immediate alerts if suspicious activity is detected.
- **Challenges**: Privacy issues regarding data collection and storage, as well as concerns about surveillance overreach and potential misuse.

4. Ethical, Legal, and Privacy Considerations

While integrated biometric surveillance systems have numerous advantages, they also raise significant ethical, legal, and privacy concerns. These include:

- **Data Privacy**: Biometric data is highly sensitive, and its collection, storage, and use must comply with data protection laws such as GDPR (General Data Protection Regulation) in Europe [20]. There are concerns over the potential for misuse or unauthorized access to biometric data.
- **Surveillance Overreach**: In some cases, the widespread use of biometric surveillance systems may lead to a "surveillance state," where individuals' movements and activities are monitored excessively, raising concerns about civil liberties.
- **Bias and Discrimination**: Studies have shown that biometric recognition systems can be biased, particularly with facial recognition, where accuracy rates can differ across racial and gender groups. This can lead to potential misidentifications and discrimination.

5. Challenges

The challenges related to the permanence and uniqueness of fingerprints significantly impact the effectiveness of biometric systems. While fingerprints are generally considered unique and persistent, various factors can compromise their reliability. Addressing these challenges is crucial for enhancing the security and accuracy of fingerprint recognition systems.

5.1. Challenges of Permanence

- Skin Conditions: Diseases or conditions affecting the skin can alter the papillary lines, leading to variations in fingerprint patterns[18].
- Environmental Effects: Factors such as moisture, dirt, or temperature can distort the quality of fingerprint scans, affecting their permanence [18][19].
- Intra-Class Variability: Variations in finger placement and pressure during scanning can result in inconsistencies, complicating the matching process[22].

5.2. Challenges of Uniqueness

- Lack of Systematic Studies: There is insufficient empirical evidence supporting the uniqueness of fingerprints over time, raising concerns about their reliability [23].
- Fingerprint Alteration: Techniques to obfuscate or alter fingerprints can significantly reduce matching accuracy, posing a threat to security systems [23][24].

Despite these challenges, ongoing research aims to develop more robust fingerprint recognition systems that can effectively address these issues, ensuring better security and user trust. However, the potential for variability and manipulation remains a critical concern in the field of biometrics.

Voice recognition technology faces significant challenges in terms of security and accuracy, primarily due to environmental variability, voice changes, and emerging threats. These challenges hinder the effectiveness of voice authentication systems, which are increasingly utilized for secure transactions and personal device access.

5.3. Environmental Variability

- Voice recognition systems often struggle with background noise and varying acoustic conditions, which can lead to misidentification or failure to authenticate users [25].
- Changes in the speaker's environment, such as different locations or noise levels, can significantly impact recognition accuracy[26].

5.4. Voice Variability

- Factors such as health, emotional state, and aging can alter a person's voice, complicating the authentication process [26].
- Voice conversion techniques, while useful for anonymity, can inadvertently expose original voice features, increasing the risk of unauthorized access [27].

5.5. Security Vulnerabilities

- Voice authentication systems are susceptible to data poisoning attacks, where malicious inputs can deceive deep learning models, allowing unauthorized access[28].
- The lack of robust defenses against such attacks poses a significant risk to the integrity of voice recognition systems [29].

Despite these challenges, advancements in deep learning and signal processing offer potential solutions to enhance both the security and accuracy of voice recognition systems. However, the balance between maintaining user privacy and ensuring reliable identification remains a critical concern[36]. Multimodal biometric systems significantly enhance the reliability of identity verification by integrating multiple biometric traits, which collectively address the limitations of unimodal systems[33]. This approach not only improves accuracy but also bolsters security against various vulnerabilities.

5.6. Enhanced Accuracy

- Complementary Strengths: By combining traits such as face, voice, and fingerprints, multimodal systems leverage the unique characteristics of each modality, leading to improved identification accuracy [30][31].
- Statistical Improvement: For instance, a multimodal system achieved an accuracy of 97% by fusing fingerprint, ear, and face biometrics, demonstrating the effectiveness of this approach [31].

5.7. Increased Security

- Robustness Against Attacks: Utilizing multiple biometric traits reduces the risk of spoofing and enhances resistance to attacks, as compromising multiple traits is significantly more challenging [4].
- Unique and Unforgeable Features: Traits like iris patterns and voiceprints are inherently unique, providing a higher level of security compared to traditional methods [4][32].

5.8. User Convenience

- Simplified User Experience: Multimodal systems eliminate the need for complex passwords or physical identification, streamlining the authentication process [4].

While multimodal biometric systems offer substantial benefits, they also face challenges such as privacy concerns and the need for secure data management to prevent misuse of sensitive biometric information [4].

6. Future Trends and Developments

The future of integrated surveillance systems in biometric authentication looks promising, with advancements in artificial intelligence (AI) and machine learning (ML) playing a significant role in improving accuracy and efficiency.

- **AI and ML Integration**: AI algorithms can help biometric systems learn and adapt to changing environmental factors, improving the accuracy of systems like facial recognition and fingerprint scanning. ML can also aid in detecting unusual patterns in surveillance data, improving threat detection.
- **Fusion of Biometric Modalities**: Future systems will likely use more sophisticated multi-modal biometric methods that combine several biometric traits for enhanced security. For example, integrating fingerprint, facial recognition, and iris scanning in a single system may become more commonplace.
- **Decentralized Data Management**: As privacy concerns increase, there is a move toward decentralized biometric data management, where biometric data is stored locally rather than in a centralized database. This approach ensures that individuals maintain control over their personal information.

7. Conclusion

Integrated surveillance systems leveraging biometric technologies have proven to be effective in improving security across various sectors, including transportation, government buildings, retail, and banking. The case studies explored in this paper highlight the practical applications of biometric systems in surveillance and the significant benefits they offer in terms of accuracy, efficiency, and fraud prevention. However, challenges such as privacy concerns, legal implications, and technological limitations remain, requiring careful consideration in their deployment. As technology continues to advance, the future of integrated biometric surveillance systems holds immense potential. With the incorporation of AI, machine learning, and multi-modal biometrics, these systems will become more sophisticated, offering even more secure and efficient solutions for monitoring and identity verification.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Subitha, D., Rahul, S. G., & Uddin, Md. P. (2024). Artificial Intelligence in Biometric Systems. 47–67. https://doi.org/10.1201/9781032702377-3

[2] Pasupuleti, M. K. (2024). Advanced Biometric Technologies in Forensic Science: Tools for Precision Identification and Investigation. 130–139. https://doi.org/10.62311/nesx/932168

[3] Sriman, J., Thapar, P., Alyas, A. A., & Singh, U. (2024). Unlocking Security: A Comprehensive Exploration of Biometric Authentication Techniques. 136–141. https://doi.org/10.1109/confluence60223.2024.10463322

[4] Fan, X., Wei, X., Zhao, Q., Jin, B., Zheng, Y., Zha, Z., Xiao, D., Feng, L., Wu, G., & Hu, J. (2024). Exploration on the Application of Multimodal Biometric Feature Recognition in System Access Control. https://doi.org/10.1109/csnt60213.2024.10545831

[5] Sharma, D., & Selwal, A. (2024). Biometrics. 1–18. https://doi.org/10.1201/9781032614663-1.

[6] Venkatesh, P., & Sreedharan, P. (2024). Face Recognition Based Security System. 1–6. https://doi.org/10.1109/icccnt61001.2024.10726275.

[7] Irfan, E., Jacob, C., & Resmi, R. (2024). Facial Recognition and CCTV Integration for Enhanced Security Using Deep Learning Techniques. 1–5. https://doi.org/10.1109/raics61201.2024.10689986.

[8] Shelokar, N., Surwase, P., Jadhav, R., Lohana, A., & Jaiswal, V. (2024). Facial Recognition Technology for Identifying Missing Individuals and Wanted Criminals. International Journal For Multidisciplinary Research, 6(3). https://doi.org/10.36948/ijfmr.2024.v06i03.21374

[9] Kumar, D., Kumaresan, M., & Deepak, S. (2024). Real-Time Facial Recognition in Computer Vision for Industrial Security. 1–6. https://doi.org/10.1109/acroset62108.2024.10743887.

[10] Esekhaigbe, E. J. (2016). Contributions to biometric recognition: fingerprint for identity verification. https://repository.cardiffmet.ac.uk/handle/10369/8340.

[11] Feng, F., Li, X., & Wang, L. (2016). Design and implementation of identity authentication system based on fingerprint recognition and cryptography. IEEE International Conference Computer and Communications, 254–257. https://doi.org/10.1109/COMPCOMM.2016.7924704.

[12] Rey, W. P. (2024). Enhancing MAFIS: A Study on the Usability and User Experience of the Mobile Automated Fingerprint Identification System. 30–34. https://doi.org/10.1109/icicse61805.2024.10625670

[13] Gomathy, Dr. C., Geetha, Dr. V., Bathrinathan, S. R., & Sripada, S. K. (2024). Exploring the ethical considerations of biometrics in cybersecurity. Indian Scientific Journal Of Research In Engineering And Management. https://doi.org/10.55041/ijsrem37507

[14] Choudhry, M. D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V. (2024). Security and Privacy Issues in AI-based Biometric Systems. 85–100. https://doi.org/10.1201/9781032702377-5

[15] Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. Ai & Society, 1–9. https://doi.org/10.1007/S00146-021-01199-9

[16] Lucero, B. A., Saracini, C., Mora, M., & Muñoz-Quezada, M. T. (2020). Aspectos éticos del uso de identificadores biométricos. Acta Bioethica, 26(1), 43–50. https://doi.org/10.4067/S1726-569X2020000100043

[17] Wienroth, M., & Amelung, N. (2023). 'Crisis', control and circulation: Biometric surveillance in the policing of the 'crimmigrant other.' 25, 297–312. https://doi.org/10.1177/14613557231184696.

[18] Drahanský, M., Kanich, O., & Březinová, E. (2017). Challenges for Fingerprint Recognition—Spoofing, Skin Diseases, and Environmental Effects (pp. 63–83). Springer International Publishing. https://doi.org/10.1007/978-3-319-50673-9_4.

[19] Saini, M. K., Saini, J. S., & Sharma, S. (2013). Various Mathematical and Geometrical Models for Fingerprints: A Survey.

[20] European Commission (2020). General Data Protection Regulation (GDPR).

[21] Cheng, C., Zhao, B. (2020). Iris Recognition Technology and Application Research in the Field of Public Security. In: Abawajy, J., Choo, KK., Islam, R., Xu, Z., Atiquzzaman, M. (eds) International Conference on Applications and Techniques in Cyber Intelligence ATCI 2019. ATCI 2019. Advances in Intelligent Systems and Computing, vol 1017. Springer, Cham. https://doi.org/10.1007/978-3-030-25128-4_194.

[22] Jain, A. K., Jain, A. K., Nandakumar, K., & Nagar, A. (2013). Fingerprint Template Protection: From Theory to Practice (pp. 187–214). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_8.

[23] Yoon, S. (2014). Fingerprint recognition: Models and applications.

[24] Sadhya, D., & Singh, S. (2018). Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions. Multimedia Tools and Applications, 77(12), 15113–15137. https://doi.org/10.1007/S11042-017-5095-X

[25] Prince, N. U., Masum, A. A., Abdullah, S. M., & Bhuiyan, T. (2024). Voice recognition by deep transfer learning and vision transformers to secure voice authentication. World Journal Of Advanced Research and Reviews, 23(3), 1365–1377. https://doi.org/10.30574/wjarr.2024.23.3.2781

[26] Ruda, K., Sabodashko, D., Mykytyn, H., Shved, M. M., Borduliak, S., & Korshun, N. (2024). Comparison of digital signal processing methods and deep learning models in voice authentication. Kìberbezpeka. Osvìta, Nauka, Tehnìka, 1(25), 140–160. https://doi.org/10.28925/2663-4023.2024.25.140160.

[27] Saini, S., & Saxena, N. (2023). Speaker Anonymity and Voice Conversion Vulnerability: A Speaker Recognition Analysis. 1–9. https://doi.org/10.1109/cns59707.2023.10289030.

[28] Li, K., Baird, C., & Lin, D. X. (2022). Defend Data Poisoning Attacks on Voice Authentication. IEEE Transactions on Dependable and Secure Computing, abs/2209.04547. https://doi.org/10.1109/TDSC.2023.3289446

[29] Defend Data Poisoning Attacks on Voice Authentication. (2022). https://doi.org/10.48550/arxiv.2209.04547

[30] Kerkeni, L., & Gueuret, T. (2024). Multimodal Biometric Authentication System Using of Autoencoders and Siamese Networks for Enhanced Security. Electronic Letters on Computer Vision and Image Analysis. https://doi.org/10.5565/rev/elcvia.1811.

[31] Hayat, A., Abhishek, K., KumarBhateja, A., & Pal, S. K. (2024). An Approach for Multimodal Biometric Authentication using Genetic Algorithm. 1–7. https://doi.org/10.1109/icccnt61001.2024.10725431

[32] Boda, A., & Joseph, M. K. (2023). Multimodal Biometrics for Human Identification usingArtificial Intelligence. https://doi.org/10.35940/ijese.a4278.1212123.

[33] Selsiya, K., Banumathy, D., & Madasamyraja, G. (2024). Person Authentication System Using Multimodal Biometrics. International Journal of Scientific Research in Science, Engineering and Technology, 11(3), 276–280. https://doi.org/10.32628/ijsrset24113129

[34] Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer.

[35] Phillips, P. J., et al. (2011). Overview of the Face Recognition Vendor Test (FRVT). NIST.

[36] Richards, N. M. (2018). Privacy and Technology in the 21st Century. Stanford Law Review.

[37] Attri, V.K. et al. (2024). Signature Verification Using Deep Learning: An Empirical Study. In: Nanda, U., Tripathy, A.K., Sahoo, J.P., Sarkar, M., Li, KC. (eds) Advances in Distributed Computing and Machine Learning. ICADCML 2024. Lecture Notes in Networks and Systems, vol 1015. Springer, Singapore. https://doi.org/10.1007/978-981-97-3523-5_14.