Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May, 2024, Martil, Morocco

Voice Biometric Technology: Enhancing Public Safety and Security in Smart Cities

Ikram BEN ABDEL OUAHAB
DIS Team, C3S Lab , FSTT,
University Abdelmalek Essaadi
Tangier, Morocco
ibenabdelouahab@uae.ac.ma
ORCID [0000-0003-0955-6382]

Lotfi ELAACHAK
DIS Team, C3S Lab , FSTT,
University Abdelmalek Essaadi
Tangier, Morocco
lelaachak@uae.ac.ma
ORCID [0000-0001-8437-5800]

Mohammed BOUHORMA
SSET Team, C3S Lab , FSTT,
University Abdelmalek Essaadi
Tangier, Morocco
mbouhorma@uae.ac.ma
ORCID [0000-0002-5687-5231]

Yasser A. ALLUHAIDAN
Saudi Authority for Data and Artificial Intelligence,
Kingdom of Saudi Arabia
y.alluhaidan@gmail.com

Bassam ZAFAR
Information Systems Department- FCIT,
King Abdulaziz University
Jeddah, Kingdom of Saudi Arabia
bzafar@kau.edu.sa
ORCID [0000-0001-5083-1548]

Abstract—**Voice biometric technology stands as a promising avenue for bolstering public safety and security within smart cities, as it finds application in access control, law enforcement authentication, and crime analysis. This review delves into its pivotal role, exploring the benefits, challenges, and future outlook. It underscores the technology's reliance on unique vocal traits for identity verification and emphasizes the critical importance of maintaining public safety amidst the proliferation of advanced urban technologies. While highlighting the advantages of heightened security and precision, the review also addresses pertinent concerns regarding privacy and ethical considerations associated with voice data utilization. Furthermore, it examines the hurdles of seamlessly integrating voice biometric technology into existing urban infrastructure, alongside discussions on potential advancements and the imperative need for regulatory frameworks, legal considerations, and public acceptance to ensure responsible implementation and widespread adoption. Ultimately, the review underscores the transformative potential of voice biometric technology in enhancing urban safety and security while emphasizing the necessity for comprehensive consideration of ethical, legal, and societal implications in its deployment.**

Keywords—Voice biometrics; Smart cities; Security; Privacy

I. INTRODUCTION

Various speech processing techniques are used in voice biometrics [1], [2]. One of the most well-known is speech-to-text. However, speech-to-text converts voice into text for subsequent matching against stored text. This is not strictly speaking a biometric technology as the voice itself is not being used to identify the speaker. Other techniques involve various forms of feature extraction from the voice [3], [4], [5]. For example, characteristics such as pitch, shape of the palate, or pronunciation of particular words can be analyzed and compared to a known voiceprint. Currently, speech recognition represents the most advanced area of speech processing technologies. This involves the recognition of spoken words, regardless of the speaker, and conversion into text. This technology is advanced, but not to the point where it can recognize speech as accurately as a human. This is, of course, a problem for voice recognition biometrics because of the potential for errors in the conversion of voice into text. Errors in conversion will lead to a mismatch between the speaker's voice and a stored voiceprint.

Voice biometric technology is the automated identification or verification of an individual based on their voice characteristics. The technology uses vocal "samples" to evaluate something about a speaker's identity, such as their claim to a particular identity or as a means of confirming their asserted identity. Voice biometrics allow a person to be identified based on their unique voiceprint. The voiceprint may be used to verify a person's claimed identity or to identify other instances of the person's voice [6], [7], [8]. Just as with fingerprint biometrics, voice biometrics can be used in two modes: identification and verification. In voice identification, the voice of an unknown speaker is compared against a group of known speakers to find a match. In voice verification, the voice of a person claiming a particular identity is compared to their voiceprint to determine if they are a match. If a match is found, the person is granted access.

II. THE VOICE BIOMETRIC TECHNOLOGY

A. Definition of voice biometric technology

The term "biometrics" is derived from the Greek words "bio" (life) and "metric" (to measure) [9]. Automated biometric systems have only become available over the last few decades, facilitated by the advancements made in the field of computer processing and data storage. Biometric systems are based on the use of data on an individual, provided by one or more intrinsic physical or behavioral traits [10], [11]. The available biometric systems span far and wide, with today's technological capabilities providing a means of identifying or verifying a person's claimed identity. These systems can be designed to work in conjunction with security or access control applications. With the ever-increasing fear of identity theft and the rising concerns regarding privacy and personal data security, biometric systems offer a more reliable and more secure solution as opposed to traditional token-based and knowledge-based methods. By measuring a person's physiological and behavioral characteristics, and comparing them with the stored data, it provides a positive means of identifying an individual. This is referred to as verification. Identification is another function of biometric systems; it involves the searching of a biometric database to find a match for the input. This could be in the instance of a criminal background check. Verification and identification go hand in hand with the primary objective of any biometric system, which is to establish a person's claimed identity with a certain degree of accuracy.

B. Importance of public safety and security in smart cities

During an emergency situation or when an individual needs help, the information should reach the concerned department quickly and accurately. Voice biometrics is one of the emergency systems through which the authentication and identification of an individual can be done through voice. The main feature of voice biometrics is to capture the voice sample of the person in normal situations and also to capture the voice sample when the person is in a bad or emergency situation. This voice sample is then compared and matched. If the voice sample does not match with the original voice of the person, then this data is sent to the concerned department, from where the call is made to the person to find out their situation. This feature is very useful when a person has an accident at home or somewhere outside. It can also help to identify a person when a crime is committed. The purpose of this feature is to save the person and find out what has happened to them. So, for the smart city, this is the gripping system to focus on the security of each and every individual.

The high concentration of a variety of security features in a specific place is called a smart city. Security is one of the most important factors that need to be focused on in order to make the city peaceful and attract investments. Also, the efficient and systematic use of energy resources is an important factor that needs to be considered. Development in a smart city, through the proper utilization of all resources, will also reduce the cost of living for citizens. The main purpose of the smart city is to mitigate the problems of the citizens. So, for better and efficient development of the smart city, an adaptive and automated system will be used to focus on security and saving energy resources.

C. Applications of voice biometric technology in smart cities

Voice biometric technology can be utilized for access control in smart cities, enabling secure and convenient authentication for entry into buildings, vehicles, or restricted areas. By accurately identifying individuals based on their unique vocal characteristics, voice recognition systems can replace traditional methods such as PINs, passwords, or keycards, reducing the risk of unauthorized access and enhancing overall security.

Law enforcement agencies in smart cities can benefit from voice biometric technology for authenticating the identities of individuals during investigations, interviews, or interactions with the public. Voice authentication can help verify the identity of suspects, witnesses, or victims, aiding in the prevention and resolution of crimes. Additionally, voice analysis techniques can be employed to detect emotional cues or anomalies in speech, providing valuable insights for law enforcement activities.[12], [13], [14]

Voice biometric technology can also be utilized for proactive crime prevention measures in smart cities. By analyzing patterns in voice data collected from various sources such as emergency calls, social media, or surveillance cameras, authorities can identify potential threats or suspicious behavior in real-time. This proactive approach allows for early intervention and preemptive action to mitigate risks and maintain public safety.[15], [16], [17]

III. LITTERATURE REVIEW AND DISCUSSION

Voice biometric technology can indeed enhance public safety and security in smart cities. By utilizing a reliable mobile voice disorder detection system embedded in a mobile application [18], cities can distinguish between healthy and pathological voices without transmitting user data, thus preserving privacy[19]. Additionally, the implementation of biometric technologies, including voice recognition, is crucial for meeting the demands of smart cities, improving efficiency, and ensuring citizen safety[20]. Moreover, the use of multimodal biometric techniques with optimized fuzzy genetic algorithms can significantly enhance accuracy and recognition rates in smart cities, addressing security concerns effectively[21]. Therefore, integrating voice biometrics into smart city systems can play a vital role in enhancing security measures and ensuring the well-being of citizens. A summary of the presented papers is presented in table I.

In [18], an enhanced multimodal biometric technique for a smart city that is based on score-level fusion is proposed, where a fuzzy strategy with soft computing techniques known as an optimized fuzzy genetic algorithm is used. Methods used are : Score-level fusion with optimized fuzzy genetic algorithm, in addition to the utilization of fingerprints and iris biometrics for recognition enhancement. The main contribution in this paper is the enhanced multimodal biometric technique with optimized fuzzy genetic algorithm, which improved performance in false acceptance rate, false rejection rate, and accuracy.

Moreover, in [19], a secure biometric-based authentication protocol for global mobility networks in smart cities focuses on biometric security. The main intention of this paper is to provide a secure protocol for GLOMONET in smart cities, and designs a protocol that is based on Li et al. Methods used are: Protocol based on Li et al.'s design, in addition to a formal analysis using BAN logic, performance and security comparison. Limitations of this study is that Li et al.'s protocol is not secure against proposed attacks. However, previous protocol's time complexity improved by 53%. Overall, the paper contribute by proposing innovative biometric applications and recognition techniques for smart cities, enhancing the existing knowledge in the field. They focus on improving security and privacy measures in biometric data handling, introducing secure protocols for data transfer in global mobility networks within smart cities.

Authors, in [20], proposed a reliable mobile voice disorder detection system capable of distinguishing between healthy and pathological voices by using a machine learning algorithm that is totally embedded in the mobile application, so it is able to classify the voice without the necessity of transmitting user data to or storing user data on any server. To implement the proposed solution, authors used Boosted Trees algorithm for voice disorder classification, and Rule-based approach with IFELSE rules for acoustic analysis. Therefore, limitations of this study can be cited as : security attacks and privacy violations in healthcare sector data., in addition to avoiding fixed healthy range to enhance system reliability. Overall, the main contribution in this paper remains in the use of acoustic parameters like F0, jitter, shimmer, and HNR, along with age and gender data, adds a unique dimension to voice disorder identification The application of Boosted Trees algorithm in distinguishing between healthy and pathological voices showcases a novel method for voice disorder classification.

In [22], the authors developed a voice biometric framework based on Convolutional Neural Network Depthwise Separable Convolution (DSC) model and the fusion of Discrete Wavelet Transform (DWT) and Mel Frequency Cepstral Coefficients (MFCC). The main contribution consists of Developing voice biometric framework with CNN DSC model. Fusion of DWT-MFCC methods for improved security performance. However, this solution required high computational costs, and burden of training parameters. To sum up, Voice biometric technology, specifically the CNN DSC model with DWT-MFCC fusion, enhances security by accurately identifying users. It can improve public safety in smart cities by providing efficient and secure identification methods.

This work [23] explores an authentication algorithm to address requirements of such memory restricted apps, and a novel computationally efficient feature extraction approach is employed over the region of interest using an efficient variation of conventional local binary pattern. Authors made feature extraction using a variation of local binary pattern, and dominant bit-plane construction for texture pattern computations. The main contribution remains in the proposition of an authentication algorithm for memory-restricted biometrics apps, with a novel feature extraction approach for unconstrained identity verification. As a result, up to 99.5% authentication accuracy achieved in unconstrained environment. Tested on UBIRISv2 database and periocular images from various devices. However, limitations are : Memory restrictions in biometrics apps, Reduced template size for unconstrained authentication.

Another application of voice biometrics is presented in [24], as a door access control system that makes use of voice recognition algorithms is proposed, where attributes of a speech are extracted and stored in a database during the training phase and a user is given access if a match is detected. They used speech recognition biometrics technology, voice recognition algorithms and vocal models. Authors aims to improve security with voice recognition for door access control system and overcoming vulnerabilities of traditional biometric technologies for enhanced security. Since Traditional biometric systems are vulnerable to hacking. Also, physical harm can bypass fingerprint, iris, and facial recognition. Voice biometrics is the best yet solution.

This paper [25] describes how Safe Citizen was conceived through Design Thinking as means of perceiving the real needs of population, and details the main functionalities offered by Safe Citizen. The paper propose a Safe Citizen which is a mobile app for public safety through citizen engagement. Aims to improve communication between public safety agencies and population. Furthermore, limitation of this study are : lack of technological solutions for smart public security in cities, and the limited focus on smart public security in smart city development.

TABLE I. SUMMARY OF LITTERATURE REVIEW

Ref.	***Methods***	***Database***	***Results***	***Pros & cons***
[18]	Fuzzy genetic algorithm. Fingerprints and iris biometrics	CASIA Iris V3 dataset FVC2006 fingerprint dataset	Accuracy = 99.88% Equal error rate = 0.18%	Enhanced accuracy, recognition rate for smart cities, optimized performance.
[19]	Protocol based on Li et al.'s design. BAN logic.	*NaN*	Improved time complexity by 53% compared to previous protocol	Enables sharing secret key in 6.1 ms with 428 bytes overhead.
[20]	Boosted Trees algorithm. Compared with : SVM, DT, NB and KNN.	MEEI, SVD, VOICED databases used for voice disorder classification. Dataset includes 2003 voice samples, 796 healthy	Accuracy = 84.5% Sensitivity = 82.9% Specificity = 86.2% Precision = 85.7% AUC = 0.91	*Pros*: Reliable mobile voice disorder detection system using machine learning. *Cons*: Potential security attacks or privacy violations in healthcare sector.

		and 1207 pathological.		
[22]	CNN Depthwise Separable Convolution model. Fusion of DWT and MFCC methods	Voice data	CNN DSC model reduced training parameters to 364,506. Speaker recognition achieved 99.25% accuracy, 97.14% precision	*Pros :* The CNN DSC model has reduced the amount of training parameters, leading to faster training process time. *Cons:* The burden of high computational costs may still be a concern despite the improvements in performance.
[23]	local binary pattern, dominant bit-plane construction for feature extraction	UBIRISv2	Accuracy = 99.5%	Biometrics offers a smart solution for city safety by enabling instant identity recognition and verification .
[24]	Speech recognition, Voice recognition using vocal models	*NaN*	Design of a door access control system using voice recognition algorithms. Testing and training phases for voice biometrics technology.	Voice biometric technology can enhance public safety and security in smart cities by providing precise and swift access control systems, reducing vulnerabilities associated with traditional biometrics.
[25]	Design Thinking process Partnership between government and academia	*NaN*	Developed through Design Thinking methodology.	Citizen engagement, timely information sharing, support for police operations.

IV. Conclusion

The papers discuss various biometric applications in smart cities, including facial recognition, emotion detection, and voice disorder identification. While one paper focuses on an enhanced multimodal biometric recognition approach using a fuzzy genetic algorithm, another proposes a secure biometric-based authentication protocol for global mobility networks.

Both papers emphasize the importance of security and privacy in biometric data handling, with one paper highlighting the need for secure data transfer in smart cities. The papers present results showing improved accuracy rates and performance metrics in biometric recognition systems for smart cities.

To conclude, the integration of biometric technologies in smart cities offers innovative applications like reconstructive facial aging models and gait analysis for healthcare monitoring. The use of an optimized fuzzy genetic algorithm for multimodal biometric recognition leads to significant improvements in accuracy rates for smart city environments. Finally, the proposed secure biometric-based authentication protocol ensures data integrity and confidentiality in global mobility networks within smart cities .

One of the primary benefits of implementing voice biometric technology in smart cities is enhanced security and accuracy in authentication processes. Unlike traditional authentication methods such as passwords or keycards, which can be easily compromised or stolen, voice recognition relies on unique physiological traits that are difficult to replicate. This increases the reliability of identity verification and reduces the risk of unauthorized access or identity fraud.

Despite its advantages, voice biometric technology raises significant privacy concerns and ethical considerations. The collection and storage of voice data for authentication purposes raise questions about individual privacy rights and data protection. There is also the risk of misuse or unauthorized access to sensitive voice data, leading to potential breaches of privacy or discrimination. Additionally, concerns regarding consent, transparency, and accountability in the use of voice biometrics must be addressed to ensure ethical deployment and responsible governance.

Another challenge of implementing voice biometric technology in smart cities is the integration with existing infrastructure and systems. Seamless integration with other technologies such as IoT devices, surveillance cameras, and data analytics platforms is essential for maximizing the effectiveness of voice recognition systems in enhancing public safety and security. However, interoperability issues, compatibility constraints, and resource limitations may hinder the smooth integration of voice biometric solutions with existing smart city infrastructure.

V. Future prospects and considerations

A. *Potential advancements in voice biometric technology*

Looking ahead, ongoing advancements in voice biometric technology hold promise for further improving public safety and security in smart cities. Research and development efforts are focused on enhancing the accuracy, reliability, and usability of voice recognition systems through innovations in machine learning, signal processing, and sensor technologies. Future advancements may also include the integration of multi-modal biometric systems that combine voice recognition with other modalities such as facial recognition or behavioral biometrics for enhanced security.

B. *Regulatory frameworks and legal implications*

As voice biometric technology continues to evolve and proliferate in smart cities, there is a need for robust regulatory frameworks and legal frameworks to govern its use and protect individual rights. Regulatory bodies must establish guidelines for the collection, storage, and processing of voice data, ensuring compliance with data protection laws and safeguarding against potential abuses. Additionally, clear legal frameworks are needed to address issues such as consent, transparency, accountability, and liability in the deployment of voice biometric systems in public spaces.

C. *Public acceptance and trust in voice biometric systems*

Public acceptance and trust in voice biometric systems are critical for their successful implementation and adoption in smart cities. To gain public trust, stakeholders must address concerns related to privacy, security, and reliability through transparent communication, education, and engagement initiatives. Demonstrating the effectiveness, usability, and benefits of voice biometric technology in enhancing public safety and security can help build confidence and acceptance among residents, businesses, and policymakers. Additionally, ensuring inclusivity and accessibility in the design and deployment of voice recognition systems is essential for fostering trust and acceptance across diverse communities.

Future Research Directions and Unanswered Questions based on literature review :

- ***Exploration of Deep Learning Algorithms:*** Future research could compare the classification accuracy of the Boosted Trees algorithm used in voice disorder detection with other deep learning algorithms to assess performance improvements.
- ***Evaluation of Mobile System Reliability***: Further studies are needed to test the reliability of mobile systems for voice disorder detection on various Android devices.
- ***Enhancement of Biometric Fusion Techniques***: Research could focus on refining multimodal biometric fusion techniques using advanced algorithms like the optimized fuzzy genetic algorithm to further improve accuracy rates.

References

[1] A. Mehrish, N. Majumder, R. Bharadwaj, R. Mihalcea, et S. Poria, « A review of deep learning techniques for speech processing », *Inf. Fusion*, vol. 99, p. 101869, nov. 2023, doi: 10.1016/j.inffus.2023.101869.

[2] A. Chhabra et D. K. Vishwakarma, « A literature survey on multimodal and multilingual automatic hate speech identification », *Multimed. Syst.*, vol. 29, nº 3, p. 1203-1230, juin 2023, doi: 10.1007/s00530-023-01051-8.

[3] T. Zhang, L. Lin, et Z. Xue, « A voice feature extraction method based on fractional attribute topology for Parkinson's disease detection », *Expert Syst. Appl.*, vol. 219, p. 119650, juin 2023, doi: 10.1016/j.eswa.2023.119650.

[4] P. Rashmi et M. P. Singh, « Convolution neural networks with hybrid feature extraction methods for classification of voice sound signals », *World J. Adv. Eng. Technol. Sci.*, vol. 8, nº 2, p. 110-125, 2023, doi: 10.30574/wjaets.2023.8.2.0083.

[5] « Human Voice Analysis to Determine Age and Gender | IEEE Conference Publication | IEEE Xplore ». Consulté le: 9 avril 2024. [En ligne]. Disponible sur: https://ieeexplore.ieee.org/abstract/document/10111890

[6] J. Deng, Y. Chen, Y. Zhong, Q. Miao, X. Gong, et W. Xu, « Catch You and I Can: Revealing Source Voiceprint Against Voice Conversion », présenté à 32nd USENIX Security Symposium (USENIX Security 23), 2023, p. 5163-5180. Consulté le: 9 avril 2024. [En ligne]. Disponible sur: https://www.usenix.org/conference/usenixsecurity23/presentation/deng-jiangyi-voiceprint

[7] S. Gui, C. Zhou, H. Wang, et T. Gao, « Application of Voiceprint Recognition Technology Based on Channel Confrontation Training in the Field of Information Security », *Electronics*, vol. 12, nº 15, Art. nº 15, janv. 2023, doi: 10.3390/electronics12153309.

[8] A. Babu, E. Raoul, G. Kassahun, I. Dufour, D. Mandal, et D. Thuau, « Programmable Polymeric-Interface for Voiceprint Biometrics », *Adv. Mater. Technol.*, vol. 9, nº 4, p. 2301551, 2024, doi: 10.1002/admt.202301551.

[9] M. Sharif, M. Raza, J. H. Shah, M. Yasmin, et S. L. Fernandes, « An Overview of Biometrics Methods », in *Handbook of Multimedia Information Security: Techniques and Applications*, A. K. Singh et A. Mohan, Éd., Cham: Springer International Publishing, 2019, p. 15-35. doi: 10.1007/978-3-030-15887-3_2.

[10] E. Koffi, « VOICE BIOMETRICS FUSION FOR ENHANCED SECURITY AND SPEAKER RECOGNITION: A COMPREHENSIVE REVIEW », *Linguist. Portf.*, vol. 12, nº 1, avr. 2023, [En ligne]. Disponible sur: https://repository.stcloudstate.edu/stcloud_ling/vol12/iss1/6

[11] « Voice Biometrics & Verification | Voice Authentication | ID R&D ». Consulté le: 27 novembre 2023. [En ligne]. Disponible sur: https://www.idrnd.ai/voice-biometrics/

[12] R. M. Fawzy, « BIOMETRIC CITIZENS in smart cities: Re-evaluating citizens' conceptualizations in smart cities policies as extended metaphorical arguments », *J. Lang. Polit.*, vol. 23, nº 2, p. 283-305, mars 2024, doi: 10.1075/jlp.22097.faw.

[13] S. Gupta et B. Crispo, « Usable Identity and Access Management Schemes for Smart Cities », in *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*, T. Dimitrakos, J. Lopez, et F. Martinelli, Éd., Cham: Springer International Publishing, 2023, p. 47-61. doi: 10.1007/978-3-031-16088-2_3.

[14] C. Catlett, J. Portugali, et V. Venkatakrishnan, « Privacy and trust in artificially intelligent cities », in *The Crisis of Democracy in the Age of Cities*, Edward Elgar Publishing, 2023, p. 167-183. Consulté le: 9 avril 2024. [En ligne]. Disponible sur: https://www.elgaronline.com/edcollchap/book/9781803923055/book-part-9781803923055-18.xml

[15] V. S. Pineda, « Emerging Trends in Cities of Tomorrow », in *Inclusion and Belonging in Cities of Tomorrow: Governance and Access by Design*, V. S. Pineda, Éd., Singapore: Springer Nature, 2024, p. 111-132. doi: 10.1007/978-981-99-3856-8_6.

[16] P. Mishra et G. Singh, « Artificial Intelligence for Sustainable Smart Cities », in *Sustainable Smart Cities: Enabling Technologies, Energy Trends and Potential Applications*, P. Mishra et G. Singh, Éd., Cham: Springer International Publishing, 2023, p. 119-142. doi: 10.1007/978-3-031-33354-5_6.

[17] B. F. G. Fabrègue et A. Bogoni, « Privacy and Security Concerns in the Smart City », *Smart Cities*, vol. 6, nº 1, Art. nº 1, févr. 2023, doi: 10.3390/smartcities6010027.

[18] V. Rajasekar *et al.*, « Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm », *Sci. Rep.*, vol. 12, nº 1, Art. nº 1, janv. 2022, doi: 10.1038/s41598-021-04652-3.

[19] M. Ghahramani, R. Javidan, et M. Shojafar, « A secure biometric-based authentication protocol for global mobility networks in smart cities », *J. Supercomput.*, vol. 76, nº 11, p. 8729-8755, nov. 2020, doi: 10.1007/s11227-020-03160-x.

[20] L. Verde, G. De Pietro, M. Alrashoud, A. Ghoneim, K. N. Al-Mutib, et G. Sannino, « Leveraging Artificial Intelligence to Improve Voice Disorder Identification Through the Use of a Reliable Mobile App », *IEEE Access*, vol. 7, p. 124048-124054, 2019, doi: 10.1109/ACCESS.2019.2938265.

[21] E. Farazdaghi, M. Eslahi, et R. El Meouche, « AN OVERVIEW OF THE USE OF BIOMETRIC TECHNIQUES IN SMART CITIES », *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. XLIV-2-W1-2021, p. 41-45, avr. 2021, doi: 10.5194/isprs-archives-XLIV-2-W1-2021-41-2021.

[22] H. Isyanto, A. S. Arifin, et M. Suryanegara, « Fast and Accurate Voice Biometrics with Deep Learning Algorithm of CNN Depthwise Separable Convolution Model and Fusion of DWT-MFCC Methods », *J. Ilm. Tek. Elektro Komput. Dan Inform.*, vol. 8, nº 3, Art. nº 3, oct. 2022, doi: 10.26555/jiteki.v8i3.24515.

[23] D. R. Ambika, K. R. Radhika, et D. Seshachalam, « Identity Verification Using Biometrics in Smart-Cities », in *Smart Cities Performability, Cognition, & Security*, F. Al-Turjman, Éd., Cham: Springer International Publishing, 2020, p. 169-199. doi: 10.1007/978-3-030-14718-1_9.

[24] V. Gupta, S. Garade, S. Kothekar, D. Meshram, S. Wankhede, et Prof. R. Pote, « An Investigative Study of Voice Functioned Smart Door Lock System », *Int. J. Res. Publ. Rev.*, vol. 04, nº 01, p. 1920-1924, 2023, doi: 10.55248/gengpi.2023.4154.

[25] B. Moreira, N. Cacho, F. Lopes, et E. Cavalcante, « Towards civic engagement in smart public security », in *2017 International Smart Cities Conference (ISC2)*, sept. 2017, p. 1-6. doi: 10.1109/ISC2.2017.8090818.