Biometrics in the World of Electronic Borders

George Kumi Kyeremeh[1], M. Abdul-Al,.[1] , Nabeel Abduljabbar, R. Qahwaji and R.A. Abd-Alhameed[1],
Faculty of Engineering and Informatics, University of Bradford[1], Bradford, BD7 1DP, UK,
G.K.KYEREMEH@BRADFORD.AC.UK; M.Abdul.Al@bradford.ac.uk; n.a.abduljabbar3@bradford.ac.uk;
R.A.A.Abd@bradford.ac.uk; R.S.R.Qahwaji@bradford.ac.uk

ABSTRACT

Recently, the demand for border crossing has increased massively, with the aim to increase the processing and clearance speed at border crossing points (BCP). The attempt to improve travel convenience, Border Cross Point (BCP) output and national security result in automated border control (ABC) with biometric technology having a major effect on the efficiency, and safety of the control processes. The border processing of BCP can be increased by automating biometric recognition and facilitated by clearance procedures. This paper discussed the two structures of an e-gate (ABC) and a prospective benefit of biometrics to the EU border in terms of accuracy, integrity, robustness, and efficiency. Challenges posed by biometrics in border control systems were identified and recommendations such as multimodal systems and smart systems with AI and machine learning were suggested to assist travelers to cross border points faster.

Keywords: Automatic Border Control (ABC), Electronic gate (e-gate), Infrared (IR), Border cross points (BCP), Machine readable zone (MRZ).

INTRODUCTION

In the conception of modern border security solutions, biometric technology has become a central focus. Biometric technologies refer to techniques of identifying and verifying people's identity according to their physiological or behavioural traits. Biometric examples include fingerprints, faces, iris. Recently, there has been a great deal of multidisciplinary focus due to the increasing use of technology in border control and in particular the application of biometric identification technology for identification and verification [1], [2]. The traditional method of identification checks by immigration officials is subject to limitations by security personnel who may have time pressure problems and security threats such faked documents.

Automated border management (ABC) is the use of automated or semi-automated systems, without the human interaction that can verify the identification and permission of visitors to cross borders with Border cross points (BCPs)[3] [4]. ABC systems which use biometrics for identification is an integral part of the solution together with monitoring systems. They serve as support for the border police to decide on passengers biological and physiological characteristics through computerised identification, verification, and cross-check of individuals. Identification is a procedure to identify who a person is while Verification is a procedural to verify if someone is who you claim to be [5]. This paper will discuss the advances and research trends with (ABC).

In contrast, biometric technologies can lead to several human rights problems and disputes and may pose ethical, social, and legal challenges. Protection of personal data is also an issue, particularly when biometrics are held in centralised systems. The ostensible relationship between biometric features and persistent personal data storage of persons is also a major concern for biometrics technology. The close connection between personal information and biometrics can both have beneficial and detrimental repercussions on people and on society [6]. Recent research on biometrics [7] has shown that personal information including gender, age, ethnicity, and even important health issues can be disclosed. Such confidential information in the context of border crossing enforcement could be utilised to discriminate between individuals[8],[6]. Basically there has been no ethnographic fieldwork situations in relation to ethical issues with significant exceptions to the studies by Rao and Nair of India's national biometric identification programme [9], [10], [11]and the DNA testing research by Finnish researchers [12]. Other challenges will be identified in detail.

STRUCTURAL DESIGN OF AN ABC SYSTEM

An e-gate provides passengers with access to a country. ABC process implementation requires diverse technology and biometric assistance. The system gets the electronic document of travel, biometric samples of the passenger and additional information from external systems. The system's output comprises of the traveller being granted or denied the border crossing [13].

THE LOGICAL STRUCTURE

The logical architecture of an e-Gate design largely consists of four interconnected subsystems.

I. Document Authentication System (DAS)
II. Biometric Verification System (BVS)
III. Central Systems Interface (CSI)
IV. Border guard Maintenance system (BGMS) [13]

The DAS is responsible for the verification of the document's validity and the extraction of information from the MRZ and the chip. By comparing live photos taken at the e-Gates and the document's information, the BVS is responsible for validating the identity of the traveller. The BGMS is allocated to the border control activities of the ABC system, whereas the interfaces with external systems are managed by the CSI.

The following five steps encompass the checks performed at a border crossing point:

I. Entry into the e-Gate
II. Scanning and Authentication of passport
III. Data extraction from the chip
IV. Verification of biometric identity
V. Data request from external systems
VI. Exit through the e-Gate

PHYSICAL STRUCTURE

Based on the time in which the document authentication and the biometric system function. The clearance procedure that an e-Gate executes may follow different logics, one-step process and two-step process while a three-step architecture is still under study [3].

In the one-step process, document identification and verifications take place in a single step and the traveller carries out all the essential steps within an e-gate. This e-Gate system can provide a high-speed clearing time because the passengers complete several parallel activities. The e-Gate can therefore produce greater efficiency if the traveller is properly trained on the use of the system [13]. **In the two-stage process**, The two-step process can be combined into one location or separated into two distinct locations [14]. A pre-enrolment kiosk for traveller verification and a single-door e-Gate for border crossing are common examples of the separated two-step process. The integrated two-step procedure is a hybrid approach, or a double-door system, in which the document verification component is located outside the e-Gate and biometric matching takes place within. [13].

PROSPECTIVE BENEFITS OF BIOMETRICS TO THE EU BORDER

The freedom of passengers in movement is constrained by the restricted or monitored borders to protect other fundamental rights within the border area, for example, safety, national or regional political or social interests. The Schengen Border Code and its amendment (Regulation (EU) 2016/399) establish regulations governing movement of persons across the internal and external borders of the Union [6]. The application of these regulations governs persons moving across the EU and the process of identifying and verifying at the border shall ensure that the proper individual is given entry or exit from a country. EU systems such as Visa Information System (VIS), European Asylum Dactyloscopy Database (EURODAC), Second-generation Schengen Information System (SIS II), and Entry Exit System (EES) emphatically apply biometrics in the management and control [15]. The integration of biometrics in border controls offers travellers, border control authorities and individual border guards' great benefit. Most prominent among these benefits are:

1. Accuracy - Precise identification and verification of passengers implies that genius can be appropriately recognised, and imposters ejected. The accuracy of the identification and verification depends on the illumination, the picture age, perception, fatigue, and make-up. The human border guard is normally quite efficient quickly after its shift begins, and then the officer gets fatigued easily. The use of multimodal biometrics results in a larger average accuracy throughout as well as makes it possible for personal data to be cross checked more accurately [16].
2. Integrity - The identification integrity is the capacity to certify that the information obtained is not altered from the collected data and its components by the issued institution. The use of biometrics improves the reduction of fraud identification since processes is not human intervened. The use of biometrics eliminates a considerable

threat to integrity, facing the border guards and benefitting the border control authority[8].

3. Robustness - Compared to border control systems consisting of human agents solely, biometric systems are straightforward to use in terms of maintain, upgrade, redeploy or decommission
4. Efficiency - The (ABC) gates' process capacity is sustained as they are not worn over time. ABC performs an objective repeatable set of tests, and documents verification can be faster and more accurate to complete than identical human controls, leading to an increasing number of low risk passengers without compromising precision or integrity. [6].

CHALLENGES POSED BY BIOMERICS IN BORDER CONTROL SYSTEMS

Biometric authentication processes can improve user comfort but some are complex, expensive and vary in accuracy as seen in the fig 1. The detection of liveliness using anti-spoofing devices is one of the primary challenges that undermine the safety of ABC systems and to delude biometric recovery systems as impostors may employ many strategies[17]. For example: facial impressions, imitation gelatine or silicone fingers, synthetic iris, and other procedures. To ensure the security of border controls, it is vital to create systems for detecting these attacks. Woefully, data of impostors on border control systems are not accessible to the public for studies. However, multiple studies have shown the susceptibility to spot attacks and other detection solutions of biometric systems [18]. Biometric pattern systems must identify how closely a biometric feature presented matches a stored feature. A biometric system often must traverse challenges associated with the non-universality of biometrics (failure to enrol), limited navigation levels, mistake rate and system security. Given the error categories, these might be either false acceptances or false rejects. The default target decision limit is at an equal error rate but would be in favour of false rejects where safety is essential. A study by [19] showed that a default algorithm would "accept" an altered image as well as the original. By using the morphing image as a "bridge" between the identity and the false identity, identity fraudsters can simply use this deception tactic. The efficiency of processes and procedures in border control depends on the power of the technological solution to detect and identify false results.

Apart from the problems of functionality and efficiency, the overall acceptance of the system for deploying biometrics depends on the adequacy of the public concern. Relevant or genuine privacy intrusion and the other undesirable (temporary or lasting) effects of system, a person's or society's anxiety and conducts may avail. [20].

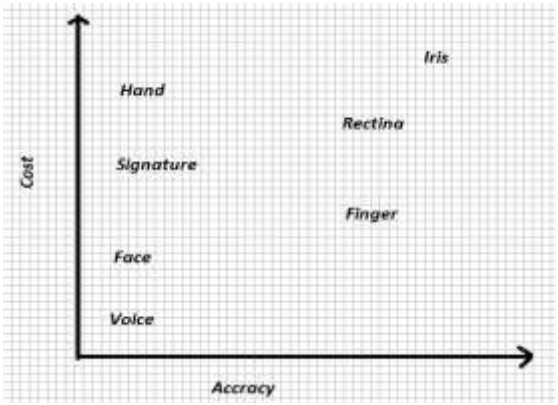

Fig 1. Comparison of the cost and accuracy of various biometrics

SUGGESTIONS TO MITIGATE THE SHORT COMINGS IN BIOMETRICS

FACE

As far as face recognition is concerned, it is important to record ICAO-friendly face images to ensure high accuracy in ABC systems. Many issues nevertheless make it difficult to acquire high-quality photographs, for example inexperience of users or problems in capturing the attention of users. To address this difficulty, solutions must be developed to train and lead the users through the acquisition process. It is also crucial to consider the height and position of the passenger to guarantee a great quality. The photographs acquired should be frontal, the centre of the image is the face and the passenger looked at the camera directly. When the image satisfies these characteristics, the system should be able to detect and detect it. Moreover, it is generally impossible to illuminate the sites where ABC systems are used by the government [21]. The biometric system must therefore deal with lighting

variations, which are the quality of the image can damage. The development of lighting solutions to offset these changes is crucial.

FINGERPRINT

Shortcomings of the fingerprint varies from quality of images acquired, how the acquired data is encrypted, through to the speed at which the images are acquired can be very slow. Developing algorithms for quality analysis which identify acquisition issues and suggest corrective action is an essential feature which can improve system usability and performance could deal with the issue of image quality. Defining standards which would ensure that systems are interoperable can provide easy access to fingerprints. They can secure the integrity and preventive access of fingerprints would be a positive direction in the step to deal with the problem posed by acquisition of data. Many sensors demand to move the finger over the buying surface for several seconds, and then wait for a frame to be of acceptable quality to avoid speed of data collection problems [22], [23].

MULTIMODAL BIOMETRICS

Using several biometric modalities aid in overcoming some of the constraints imposed by unimodal biometric systems. These systems, known as multimodal biometric systems and due to the availability of numerous, independent pieces of evidence, are believed to be more reliable [24]. For enrolment, verification, or identification, multimodal biometric systems use more than one physiological or behavioural characteristic. Because of the rise in the information available for recognition, these systems could undertake more reliable verifications of the traveller's identity [25]. A passport holder's identity verification using the face may not be successful in combating identity theft until multimodality is used. Additionally, improved matching performance would result in a better user experience as well as an increase in passenger flow efficiency. The multimodal approach to identity verification is gaining recognition in systems of ABC, given the increasing number of deployments that have begun using this technology.

INCOPERATION OF INFRARED

Infrared imaging with IR thermal sensors can make lighting adjustments more resilient and can work in dark situations. IR images may also collect additional physiological and anatomical face-related data, like a blood vessel structure and the thermal facial signature, which may be utilized by individuals as unique biometrics. The accuracy of thermal faces is rather good but there is still a need for more accuracy, because high accuracy is vital for security systems, as even the slightest mistake may influence national safety and access control. The use of multi-modal combining algorithms by comparative thermal (IR) and optical (visual) images. Recordings both optical and thermal images for identification have emerged as a potential solution to curb any anomalies in the IR imaging system and has been improved by concurrently using a single sensor of charged coupled device (CCD) and low wave infrared (LWIR) micro bolometer.

SMART SYSTEMS

The blend of a new-generation border safety technology combines multiple anatomical traits to enhance identification accuracy, while data collection processes are being performed to provide a smoother individual border crossing experience [26]. The Gitex Technology Week Dubai World Trade Centre in October 2017 exhibited a Smart Tunnel system, a tunnel design with over 80 high-tech cameras that provide high-quality images that routes passengers to their destinations. Identifying the biometrics of the individual takes occur through a process of multi-scanning. When travellers pass, biometric technology then scans face or iris with cameras while in motion. The tunnel contains a full body scanner in addition to the biometric recognition (FBS). The Smart Tunnel, like a longer version of the Smart Gates, is not closed. The system incorporates face and iris recognition, Artificial Intelligence, and machine learning technology. The aim is to make it possible for travellers to cross the tunnel easily within a few seconds without having to stamp their passports or any other interaction by humans [20].

CONCLUSION

This paper focused on ABC emerging as the innovative solution to border control and management having a great relation with

Biometrics. There are primarily four subsystems in an e-Gate that work along with the passenger clearing process: biometric check, document authentication, border guard maintenance and external systematic interface. In view of the challenges of every biometric feature, the usability of biometric systems is crucial and as a result using several biometric modalities aid in overcoming some of the constraints imposed by unimodal biometric systems. The use of multi-modal combining algorithms of thermal and optical images recordings both optical and thermal images has emerged as a potential solution to curb any anomalies in the IR imaging system and visual images. Finally, a smarter system which incorporates Artificial intelligence and machine learning to make it possible for travellers to cross border points faster without human interaction.

Acknowledgments

This project has received funding from the European Union's Horizon-MSCA-RISE-2019-2023, Marie Skłodowska-Curie, Research, and Innovation Staff Exchange (RISE), titled: Secure and Wireless Multimodal Biometric Scanning Device for Passenger Verification Targeting Land and Sea Border Control

REFEENCES

1. Dijstelbloem, H., A. Meijer, and M. Besters, The migration machine, in Migration and the new technological borders of Europe. 2011, Springer. p. 1-21.
2. Broeders, D. and J. Hampshire, Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe. Journal of Ethnic and Migration Studies, 2013. **39**(8): p. 1201-1218.
3. Frontex, R., Best practice operational guidelines for Automated Border Control (ABC) systems. European Agency for the Management of Operational Cooperation, Research and Development Unit,. https://bit. ly/2KYBXhz Accessed, 2012. **9**(05): p. 2013.
4. Amato, A., V. Di Lecce, and V. Piuri, Semantic analysis and understanding of human behavior in video streaming. 2012: Springer Science & Business Media.
5. Bhatia, R., Biometrics and face recognition techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 2013. **3**(5).

6. Abomhara, M., et al., How to Do It Right: A Framework for Biometrics Supported Border Control, in Communications in Computer and Information Science. 2020, Springer International Publishing. p. 94-109.
7. Dantcheva, A., P. Elia, and A. Ross, What else does your biometric data reveal? A survey on soft biometrics. IEEE Transactions on Information Forensics and Security, 2015. **11**(3): p. 441-467.
8. Council, N.R. and W.B. Committee, Biometric recognition: Challenges and opportunities. 2010.
9. Rao, U. and V. Nair, Aadhaar: Governing with biometrics. 2019, Taylor & Francis.
10. Rao, U., Biometric bodies, or how to make electronic fingerprinting work in India. Body & Society, 2018. **24**(3): p. 68-94.
11. Nair, V., An eye for an I: recording biometrics and reconsidering identity in postcolonial India. Contemporary South Asia, 2018. **26**(2): p. 143-156.
12. Tapaninen, A.-M., M. Halme-Tuomisaari, and V. Kankaanpää, Mobile lives, immutable facts: family reunification of children in Finland. Journal of Ethnic and Migration Studies, 2019. **45**(5): p. 825-841.
13. Labati, R.D., et al. Advanced design of automated border control gates: biometric system techniques and research trends. in 2015 IEEE International Symposium on Systems Engineering (ISSE). 2015. IEEE.
14. Labati, R.D., et al., Biometric recognition in automated border control: a survey. ACM Computing Surveys (CSUR), 2016. **49**(2): p. 1-39.
15. Kenk, V.S., et al., Smart surveillance technologies in border control. European Journal of Law and Technology, 2013. **4**(2).
16. ICAO, D., 9303-Machine Readable Travel Documents-Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs. International Civil Aviation Organization (ICAO), 2015.
17. Marasco, E. and A. Ross, A survey on antispoofing schemes for fingerprint recognition systems. ACM Computing Surveys (CSUR), 2014. **47**(2): p. 1-36.
18. Bowyer, K.W. and M.J. Burge, Handbook of iris recognition. 2016: Springer.
19. Scherhag, U., et al. Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. in 2017 International Conference of the Biometrics Special Interest Group (BIOSIG). 2017. IEEE.
20. Binder, S., A. Iannone, and C. Leibner, Biometric technology in "no-gate border crossing solutions" under consideration of privacy, ethical, regulatory and social acceptance. Multimedia Tools and Applications, 2020: p. 1-14.
21. Spreeuwers, L.J., A.J. Hendrikse, and K. Gerritsen. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport. in 2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG). 2012. IEEE.
22. Labati, R.D., et al. Quality measurement of unwrapped three-dimensional fingerprints: a neural networks approach. in The 2012 International Joint Conference on Neural Networks (IJCNN). 2012. IEEE.
23. Labati, R.D., V. Piuri, and F. Scotti. Neural-based quality measurement of fingerprint images in contactless biometric systems. in The 2010 international joint conference on neural networks (IJCNN). 2010. IEEE.
24. Jain, A.K. Biometric recognition: overview and recent advances. in Iberoamerican Congress on Pattern Recognition. 2007. Springer.
25. Jain, A.K. and A. Ross, Multibiometric systems. Communications of the ACM, 2004. **47**(1): p. 34-40.
26. Rubins, U., et al. Real-time photoplethysmography imaging system. in 15th Nordic-Baltic Conference on Biomedical Engineering and Medical Physics (NBC 2011). 2011. Springer.