DOI: 10.2507/32nd.daaam.proceedings.056

THE ROLE OF LIE DETECTION BASED SYSTEM IN CONTROLLING BORDERS

Lucie Sousedikova, Adam Malatinsky, Irena Drofova & Milan Adamek

This Publication has to be referred as: Sousedikova, L[ucie]; Malatinsky, A[dam]; Drofova, I[rena] & Adamek, M[ilan] (2021). The Role of Lie Detection Based System in Controlling Borders, Proceedings of the 32nd DAAAM International Symposium, pp.0384-0388, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-33-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/32nd.daaam.proceedings.056

Abstract

Security engineering refers to the latest techniques and methods used to protect large numbers of people concentrated in public crowded places every day. Such a new modern method represents the Intelligent Portable Border Control System (iBorderCtrl) based on lie detection. This paper describes and analyses this automated deception detection border security system developed mainly for airport security but also for the control of the land border crossing points as roads, walkways, or train stations. The system is built using advanced and high-performance deep learning models with the aim of effectively prevent any threats or potentially dangerous situations from arising or entering the country.

Keywords: Border Control; Deception Detection; Lie Detection; Analysis.
.

1. Introduction

Nowadays, border agencies come under considerable pressure with continuous traffic growth, combined with the increased threat of terrorist attacks and refugee crisis. That is why the areas of borders and migration management have become more and more prominent as sites of experimentation and investment. The European Commission has set aside a proposed €34.9 billion for border control and migration management between 2021 and 2027 (Gallagher & Jona, 2019). Recently, it was developed and tested new border control system called Intelligent Portable Border Control System (iBorderCtrl) which was funded by €4.5 million under the EU Horizon 2020 program [2].

The iBorderCtrl is a comprehensive system that consists of a two-stage procedure, designed to reduce cost and time spent per traveller at the border crossing station. It is an innovative automated border security system that detects deception based on lie detection, facial recognition technology, and the measurement of human micro gestures and non-verbal behaviour due to an artificial intelligence system known as an avatar. Although various works that used artificial neural networks have been done [3], [4] they have been too limited. Currently, there is a lot of publications describing the iBorderCtrl project [5]. This paper examines a recently drafted border control system by using critical analysis and highlights its main shortcomings.

2. Critical Analysis Framework

In this research, the iBorderCtrl system is analysed by using critical analysis which depicts strengths but above all limits of the system. Figure 1 introduces the method of critical analysis and shows its architecture for understanding. As shown, the outcome of the critical analysis is the entire evaluation of the system.

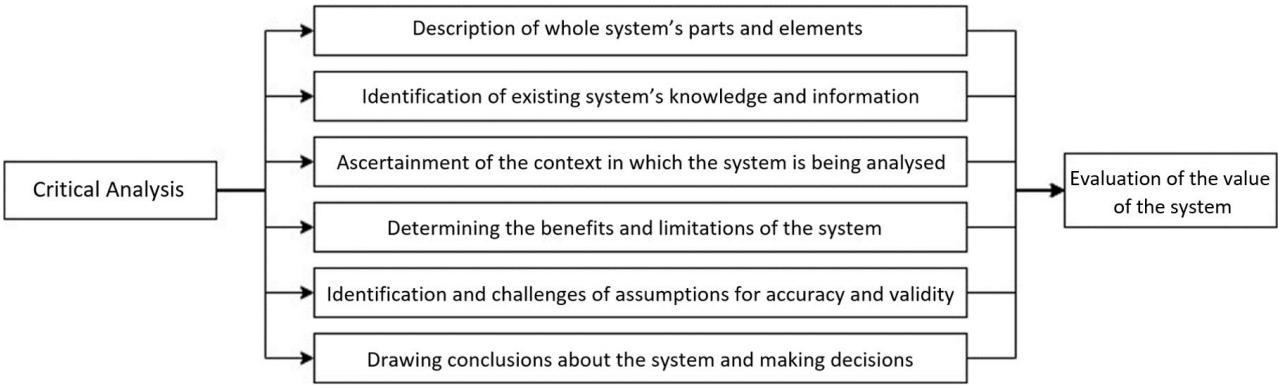

Fig. 1. Critical Analysis Framework

3. Technical Framework

The iBorderCtrl specific objective is to significantly increase traveller throughput at the borders in reduced time and at the same time enhance the security by bringing together many states of the art hardware and software technologies. This section provides a general overview of the iBorderCtrl's interfaces and subsystems with their technical description.

Fig. 2. Intelligent Portable Border Control System [6]

The system has three different interfaces, one for each type of user, and different modules for processing the gathered information:

- Traveller User Application for the traveller
- Border Guard User Application for the border guard agents
- Border Manager User Application for the border guard managers [7].

The modules that complete the system are in charge of processing the information, analyse the possible risks associated and provide useful information to the border guards to manage more effectively the Border Crossing process. The main modules composed the overall system solution are the following:

- **The Automatic Deception Detection System (ADDS).** During the pre-travel stage, ADDS requires each traveller to undertake an interview with an avatar, a sophisticated artificial intelligence system utilizing non-verbal micro-gestures to detect deception. Figure 1 presents the ADDS architecture. Each traveller has a QR code that uses throughout the interview. Control is passed from the Traveller User Application to ADDS using an iframe, at which point ADDS requests sufficient information to be able to ask 16 questions by the actual border guard in real-life crossing scenario. ADDS interviews with an avatar (male or female) that utilizes three attitudes (puzzled, neutral, positive) depend upon the deception score of the last question answered. ADDS requests to the avatar database to receive the requested corresponding Avatar video and updates the local ADDS database respectively. At the end of the interview the video frames, questions, and interview scores are uploaded to the iBorderCtrl databases to be used by the RBAT, FMT, and BCAT modules [6], [8].

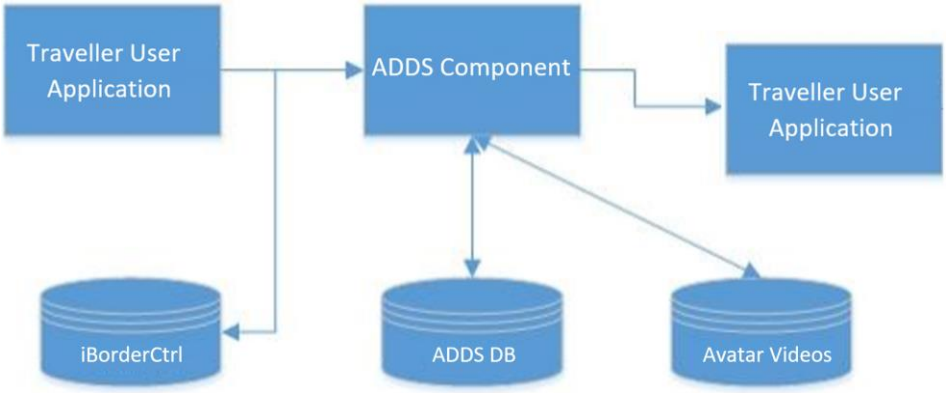

Fig. 3. ADDS Modul [6]

- **The Risk Based Assessment Tool (RBAT)** calculates and manages-traveller related risks in the border check procedure. It is a robust and flexible tool to support the decision-making process of the border authorities.
- **The Integrated Border Control Analytics Tool (BCAT)** includes advanced analytics methodologies for border managers. BCAT analysis detects illicit activities or patterns of behaviour associated with illegal activities. It also evaluates the effectiveness of each iBorderCtrl system.
- **The Biometric Module** consists of the fingerprint and palm vein modules validating the identification of the traveller. The aim of both modules is to compare the fingerprints and palm vein images to relevant information stored in European databases. Then the risk scores according to the match percentage through the central server software for matching are provided and forwarded to the iBorderCtrl database for the RBAT overall risk score calculation and assessment.
- **The Face Matching Tool (FMT)** is the facial recognition system for iBorderCtrl which is used both at the pre-registration and the border crossing phase**.**
- **The Hidden Human Detection Tool (HHD)** detects any hidden people inside various vehicles. For detection are used a radar/electromagnetic or an acoustic sensor depending on detecting space. The radar sensor is suited for the detection of all non-metallic spaces and compartments. In contrast, the acoustic sensor is used mainly for metallic cargo containers. Both types of sensors are small, and light weighted and support the Border Guard.
- **The Document Authenticity Tool (DAAT)** is used during the pre-registration as well as the border crossing stage. At the pre-registration stage, DAAT deals with the information (passport, visa, ID, residence permit) provided by the traveller using the Traveller User Application. At the border crossing point, the border guard uses the document scanner integrated into the Portable Unit to scan travel documents. The DAAT system checks the security features of documents and assesses the validation of documents and detects its counterfeiting.
- **The External Legacy and Social interfaces systems (ELSI)** checks the traveller's information from legacy systems (SIS II etc.) [6], [9].

4. Border Control Procedure

The iBorderCtrl changes the traditional approach followed in border management with a new one based on the integration of advanced technologies for data analysis for Border Guards and the two-stage procedure for the travellers:

- **Pre-registration stage** when all travellers are linked to any pre-existing authority data and through the Traveller User Application (web, mobile application), that verifies the authenticity are able to update their personal and travel information, upload travel-related documents, see expected traffic statistics regarding the selected country and border control point, pass an avatar interview conducted by ADDS. During the interview is filmed by his/her video camera and computer software obtains his/her micro-gestures to detect deceptive behaviour. The FMT is used and the traveller´s passport photo is compared to a short video sequence of the traveller.
- **The border crossing stage** when all registered documents and information are re-evaluated and the security controls are performed by a portable iBorderCtrl unit which consists of the devices needed to capture information (camera, fingerprint sensor, document reader, etc.) and provides the Border Guard Application for border guards. The Traveller User Application verifies the authenticity and truth of information forwarded. At this stage, the travellers present themselves by QR code to the border guard could obtain his/her personal information and the risk assessment score through the Border Guard User Application bringing all analytic results from each technology together to identify risks to the border guard. It enables overall evaluation of the traveller as well as highlighting specific potential issues the agent should focus on. In the end, like in the pre-registration phase, the risk is calculated. Furthermore, biometric checks (face matching, fingerprints, palm vein) and hidden human detection (crossing with the vehicle) take place. The face-matching tool performs the validation of the identity of the traveler to assign the risk of deception. It includes three different checks:

- Matching the images taken by the portable unit's camera and the high-definition image obtained from the passport or any external system such as VIS.
- Measuring the risk that the person appearing in the documents is the same one that undertook the avatar interview.
- Measuring the risk that the person at the border crossing point (images taken by the camera of the portable unit) is the same one that performed the interview during the pre-travel stage. [6], [9], [10].

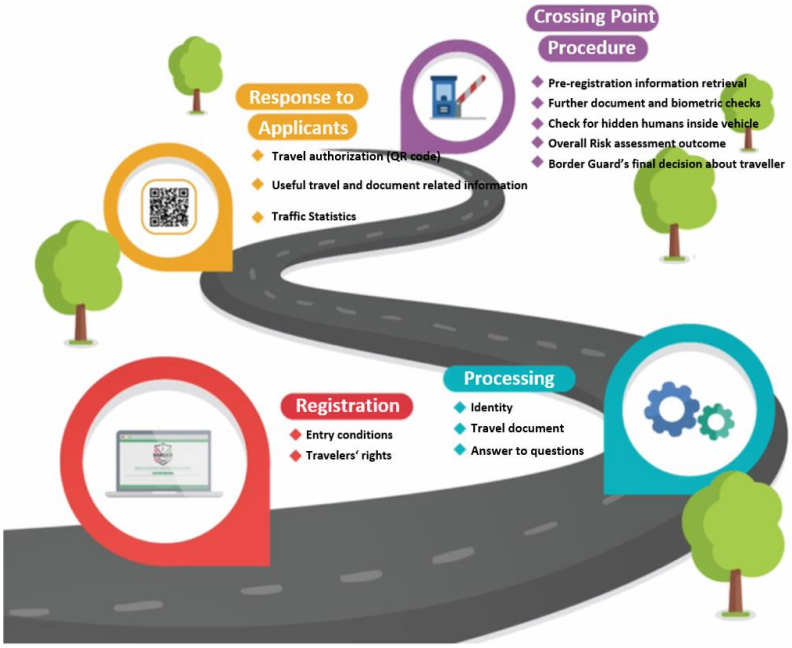

Fig. 4. Border Control Procedure [7]

5. Critical Analysis

The iBorderCtrl system solution changes the traditional approach followed in border management with a new one based on the two-stage procedure for travellers and the integration of modern technologies for data analysis. Since the end of the project testing phase, the iBorderCtrl is still considered experimental. This section provides a critical analysis of this system and outlines its benefits and limitations.

The iBorderCtrl system provides a wide range of capabilities and advantages such as:

- Document validation
- Face recognition
- Hidden human detection
- Data Analytics and statistics
- Provide early-warning capabilities due to risk assessment
- Three different interfaces
- Portable unit with Commercial-Off-The-Shelf technologies
- Easily expansion with new technologies or functionalities
- The possibility of integrating the similar functionalities of the new ETIAS system
- New two-stage procedure for border crossing
- Extend the capabilities of taking the border crossing procedure to where the travellers are (bus, car, train, etc.) instead of moving the travellers to where the checking booth is [7].

Since the end of the project testing phase, the iBorderCtrl is still considered experimental. Although it has its benefits, there is still a lot of shortcomings of this system:

- **Imperfect deception detection system** based on facial recognition which is still in progress in development. Currently, the system is not suitable - it is biased towards minorities and people with a range of nervous system abnormalities and correlated differences in social behaviour (attention-deficit disorder, post-traumatic stress disorder, people with depression state, or chronic pain conditions, etc.). Because researchers trained their artificial intelligence on a small sample of mostly European men, the system can discriminate against people based on their ethnic origin, and it has had a higher accuracy rate for the mentioned group.

- **Success rate of 75%** although it was assumed the success rate of 85%. On the contrary, the accuracy of the polygraph is up to over 90% according to the American Polygraph Association. But it is necessary the trained polygraph examiners who conduct time-consuming interviews that depend on the subject and the object of the investigation. On the other hand, this artificial lie detector is automated and has a great potential for easy use on many people, there is still a wide scope for errors. Many reporters and journalists have already tried to test the system and however, they answered honestly to all questions, they were evaluated as liars.
- **Need to establish an extensive biometric database** called Common Identity Repository if the EU wants to implement it continent-wide.
- **Threat to freedom of thought** is in danger with this technology. That is a big question if the system can look inside people's minds, it is legal to set it as mandatory. Together with new neurological applications, this requires a new legal framework in the future to protect the old human rights as the right to mental privacy, the right to mental integrity, the right to psychological continuity cognitive liberty.

6. Conclusion

The iBorderCtrl system was designed and developed with the specific objective to significantly increase traveller throughput at the borders in reduced time as well as security in terms of significantly fewer successful crimes. The system consists of three user-friendly applications and several modules that are in charge of processing the information, analyse the possible risks associated, and provide useful information to the border guards to manage more effectively the border crossing process. Despite being considered as a new modern solution - automated, unobtrusive, and easily used, the system is still limited. The main purpose of this research was to analyse it and highlight its limitations. After the completion of the pilot phase of the iBorderCtrl in Greece, Hungary, and Latvia, the system is still considered experimental and does not prevent anyone from entering the European Union for now. However, since august 2019 everyone who crossed the borders of a member state for the first time has been already provided his/her personal data including his/her privacy data on social media. If the shortcomings of the system presented in this article were corrected, the system would represent an automated, simple, and easily used solution for faster border crossing processes of EU for third-country nationals. Every passenger could be checked quickly but carefully whilst keeping the strict regulations. In this case, the iBorderCtrl could complement existing border control technology. Also, it would facilitate the border guards' working in spotting illegal immigrants, and it would prevent crime and terrorism. But on the other hand, there is still a lot of limitations and disadvantages. For the future, research would need to use more diverse study samples, or its accuracy rates will drop for racial reasons. Also, the people´s right to privacy should be solved.

7. Acknowledgement

This work was supported by the Internal Grant Agency of Tomas Bata University in Zlin, the Department of Security Engineering, Faculty of Applied Informatics, under the project No. IGA/CebiaTech/2021/004.

8. References

[1] Gallagher, R.. & Jona, L. (2019). We Tested Europe’s New Lie Detector for Travelers—And Immediately Triggered a False Positive. The Intercept. Available from: https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/ Accessed: 2021/09/20

[2] Sánchez-Monedero, J. & Dencik, L. (2020): The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl, Information, Communication & Society, DOI 10.1080/1369118X.2020.1792530

[3] Holmes, M.; Latham, A.; Crockett, K. & O'Shea, J. D. (2017). "Near Real-Time Comprehension Classification with Artificial Neural Networks: Decoding e-Learner Non-Verbal Behavior," IEEE Transactions on Learning Technologies, Vol. 11, No. 1, pp. 5-12, 2018, DOI 10.1109/TLT.2017.2754497.

[4] Rothwell, J.; Bandar, Z.; O'Shea, J. & McLean, D. (2006). Silent talker: A new computer-based system for the analysis of facial cues to deception. Applied Cognitive Psychology. 20. 757 - 777. 10.1002/acp.1204.

[5] The iBorderCtrl (2020). Publications, Available from: Publications | iBorderCtrl Accessed: 2021/09/20

[6] The iBorderCtrl Consortium (2015). Intelligent Portable Control System, Available from: https://www.asktheeu.org/es/request/6087/response/19711/attach/4/8%20D3%202%20First%20version%20of%20tech%20tools%20and%20subsystems%20redacted.pdf?cookie_passthrough=1 Accessed: 2021-09-20

[7] The iBorderCtrl (2020). Outcomes, Available from: Publications | iBorderCtrl Accessed: 2021/09/20

[8] OrShea, J.; Crockett, K.; Khan, W.; Kindynis, P.; Antoniades, A. & Boultadakis, G. (2018). Intelligent Deception Detection through Machine Based Interviewing, Proceedings of International Joint Conference on Neural Networks, Rio de Janeiro, Brazil, ISSN 2161-4393, ISBN 978-1-5090-6014-6, pp 1-8, DOI 10.1109/IJCNN.2018.8489392

[9] The iBorderCtrl (2020). Technical Framework, Available from: Publications | iBorderCtrl Accessed: 2021/09/20

[10] Rodríguez Carlos-Roca, L.; Hupont Torres, I. & Fernandez, C.(2018). Facial recognition application for border control, Proceedings of International Joint Conference on Neural Networks, Rio de Janeiro, Brazil, ISSN 2161-4393, ISBN 978-1-5090-6014-6, pp 1-7, DOI 10.1109/IJCNN.2018.8489113