Konference Mladá věda
16. března 2021, Univerzita Tomáše Bati ve Zlíně

ANALYSIS OF ARTIFICIAL INTELLIGENCE LIE DETECTOR DEVELOPED FOR AIRPORT SECURITY

Lucie SOUSEDIKOVA, Martin HROMADA, Milan ADAMEK
Tomas Bata University in Zlin, Faculty of Applied Informatics
Nad Stranemi 4511, 760 05 Zlin, Czech Republic
l_sousedikova@utb.cz, hromada@utb.cz, adamek@utb.cz

Abstract:

Airport security is a very topical issue nowadays. Airports are characterized by a high concentration of people and increasing security demands especially related to the threat of terrorist attacks. That is why they have long been at the forefront of investments in modern technologies such as body scanners or biometric gateways. In order to ensure the highest possible safety for its passengers, the aviation industry constantly adopts new modern technologies that are able to detect crime. The Intelligent Portable Border Control System based on lie detection represents such a method. Its principles of operation, system vulnerabilities, and possibilities of its implementation at airports are discussed in this article.

Keywords: *Airport Security, the iBorderCtrl, Automated Deception Detection System, Analysis.*

1 Introduction

In recent years, terrorism and illegal immigration have shown its fatal consequences in several parts of Europe which worldwide has cost many lives and important economic losses. Following the refugee crisis and a spate of terrorist attacks in Belgium, France Spain, or Germany, Europe comes under increasing pressure to protect land borders with the purpose of tracking the movements of migrants and terrorists more effectively.

More than 700 million people annually enter the EU according to the European Commission. In addition, this number is increasing rapidly and the huge volume of travellers is pilling pressure on external borders that is make it increasingly difficult for border staff to check every passenger carefully whilst keeping the strict security regulations. The solution could be the artificial intelligence, based on lie detection technology, called Intelligent Portable Border Control System (iBorderCtrl), which was tested at airports in Hungary, Latvia, and Greece on passengers in 2018 and funded by the €4.5 million under the EU Horizon 2020 program.

The iBorderCtrl is aiming to deliver faster border crossing processes of EU for third-country nationals while enhancing the security of border control checks and facilitating the work of border guards in spotting illegal immigrants, and so contribute to the prevention of crime and terrorism.

The iBorderCtrl is aiming to deliver faster border crossing processes of EU for third-country nationals while enhancing the security of border control checks and facilitating the work of border guards in spotting illegal immigrants, and so contribute to the prevention of crime and terrorism. This system could complement existing border control technology such as Advanced Passenger Information systems and future systems such as the new Entry/Exit System centralized border management system.

The part of iBorderCtrl System is the Automated Deception Detection System including an advanced border control agent known as an avatar. The avatar conducts the interview and communicates with the traveller during pre-travel stage. Such an artificial intelligence system is able to detect a human non-verbal behaviour (NVB) which can be produced subconsciously in contrast to spoken language. Various works has been done has been done in the automated extraction of NVB from a learning system [1] to detect comprehension levels and also in detection of deception [2]. Although both of the mentioned examples have used artificial neural networks to first detect micro gesture patterns and then perform classification successfully, they have been too limited.

2 Method Section

Before conducting the analysis itself and underlining the main limitations of the iBorderCtrl System it is necessary to introduce the method of critical analysis. This section provides to understand the individual parts and outcomes of this method.

In this research, a critical analysis is used for the evaluation of the effectiveness of a particular system. It is also called system analysis. Its purpose is to carefully examine the iBorderCtrl System – to break down this system and study its parts to give the entire evaluation.

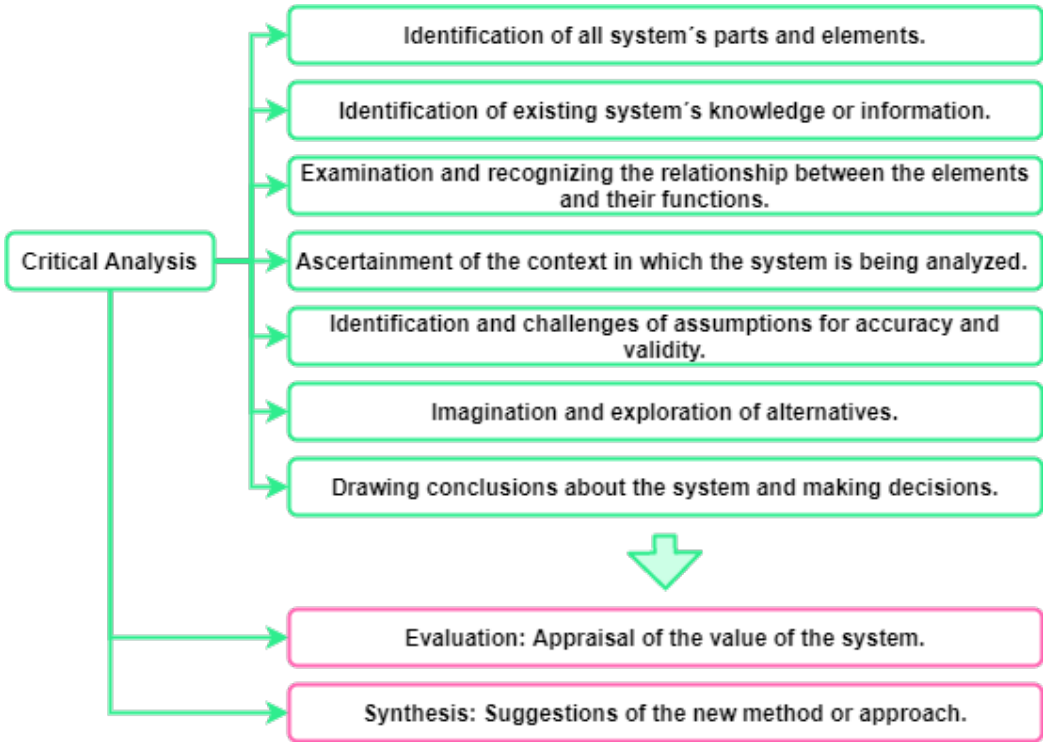

Fig. 1: The Critical Analysis Architecture. [own source]

3 The iBorderCtrl Architecture

In this section, each of the subsystems of iBorderCtrl is described. The iBorderCtrl system is composed of the following modules.

3.1 The Automated Deception Detection System

The Automated Deception Detection System known as ADDS is responsible for conducting the interview where the traveller is asked to respond to 16 questions to an embodied conversational agent referred to as an avatar. All travellers are required to undertake an interview with an avatar during the pre-travel registration. It is a sophisticated artificial intelligence system utilizing gestures and subtle non-verbal communication cues to stimulate richer responses from travellers due to detect deception. The avatar is able to adopt three attitudes (puzzled, neutral, or positive) on the basis of the deception score of the last question asked. At the conclusion of the interview, questions, interview scores and video frames are uploaded to the iBorderCtrl database to be used by the Radar & Beacon Analysis Tool (RBAT), Face Matching Tool (FMT), and Brief Cognitive Assessment Tool (BCAT). [3]

3.2 Document Authenticity Analytics Tool

Document Authenticity Analytics Tool (DAAT) deals with the verification of traveller‘s documents (passports, IDs, car licence, etc.) in a short time during the pre-travel stage as well as the border crossing stage. It checks the quality of information through document scanners, readers, and IP cameras to detect counterfeiting. The DAAT system also informs the border guard about passport security features that he should concentrate on, assess its validation, and creates a risk score.

3.3 The fingerprint and palm vein modules

The fingerprint and palm vein modules validate the identity of a traveller. By the fingerprint reader located in the portable unit is captured the sample which compares to the traveller biometric passport (RFID chip) and fingerprints stored in different national or European databases. The palm vein sensor is used as a secondary identification method because nowadays there is no palm vein database. This module should compare the biometric captured template with the biometric enrolment template previously stored. Both modules provide risk scores according to the match percentage through the central server software for matching. The results are forwarded to the iBorderCtrl database for the RBAT overall risk score calculation and assessment.

3.4 Face Matching Tool

The Face Matching Tool (FMT) is the facial recognition biometric system which is used in both the pre-travel and border crossing stage as described in the following section.

3.5 Hidden Humans Detection

If the travellers cross the borders by vehicle, at the border control point Hidden Humans Detection module (HDD) is used to detect the presence of an alive being inside vehicles or closed compartments. The detection of presence is based on the detection of the micro-movements or vital signs of the alive being (breathing, slight movements, or vibrations). The main purpose of HDD is to prevent illegal migration and trafficking. [4]

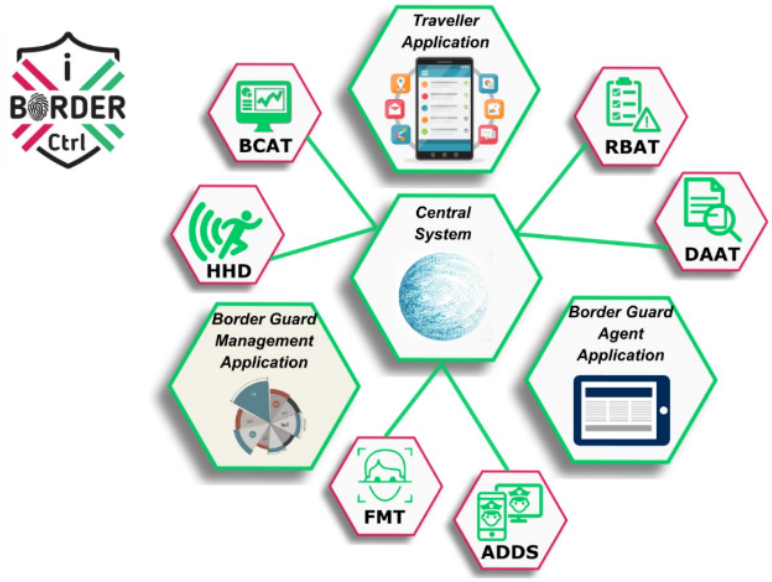

Fig. 1: The iBorderCtrl Architecture [5]

4 The two-stage procedure

The iBorderCtrl consists of a two-stage procedure designed to reduce cost and time spent per traveller at the crossing station.

4.1 Pre-Travel Stage

The Pre-Travel stage is the registration stage designed to:

- Link the traveller to any pre-existing authority data.
- Gather initial personal information, travel documents and information, and vehicle data through the Traveller User Application that verifies if the mandatory information is all completed, and check the authenticity of the uploaded travel documents.

- Perform a short automated interview with a virtual border agent (artificial figure called avatar representing a border guard) conducted by Deception Detection System (ADDS). During the avatar interview, a set of travel-related questions is asked and the false answers are detected by the system observation of non-verbal behaviour. The same questions an actual border guard may ask travellers in a real-life border crossing scenario. The traveller is filmed by using his/her video camera while computer software observes his/her facial micro-gestures to detect deceptive behaviour. Then, a face-matching tool (FMT) is conducted in which the traveller's passport photo is compared to a short video sequence of the traveller. This biometric reference is used later to check the risk of deception. [4,5]

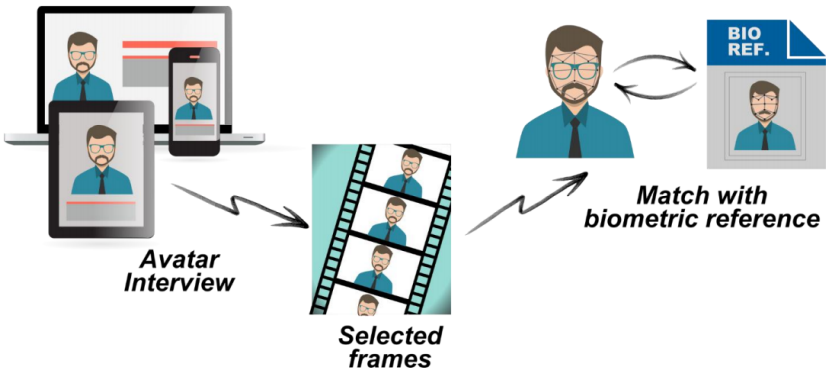

Fig. 2: FMT in the pre-travel stage [6]

4.2 The Border Crossing Stage

The Border Crossing Stage is the actual control at the border that complements registered information with the results of security controls that are performed with a portable iBorderCtrl unit. The portable unit consists of the set of devices needed to capture information (camera, fingerprint sensor, document reader, etc.) and provides the Border Guard Application for guiding the border guards in the individual steps of the defined procedure. First of all, the traveller has to present his/her QR code to the border guard could access traveller's personal information provided at the pre-travel stage and the risk assessment score. After that, the border guard verifies the authenticity of the travel documents by a portable scanning device, as well as vehicle information and proceeds to match the fingerprint reference with the traveller.

If necessary, further the advanced biometric technologies are used - the facial recognition and the palm vein technologies. The three different checks take place during the face recognition to assign the risk of deception. The first one controls that the person at the border crossing point is the same one as the one shown in the documents by drawing a comparison between the portable unit's camera and the high definition image obtained from the passport embedded RFID chip or from any external system. The second check shows if the person appearing in the documents is the same one that performed the avatar interview. And the third check compares the person at the border cross point (images taken by the camera of the portable unit) with the person that undertook the interview during the pre-travel stage.

If the traveller crosses the borders by private car, then the border check realizes the hidden human detection. All the information is analysed to provide an overall risk level to assist the border guard in deciding about the individual traveller. [4,5,6]

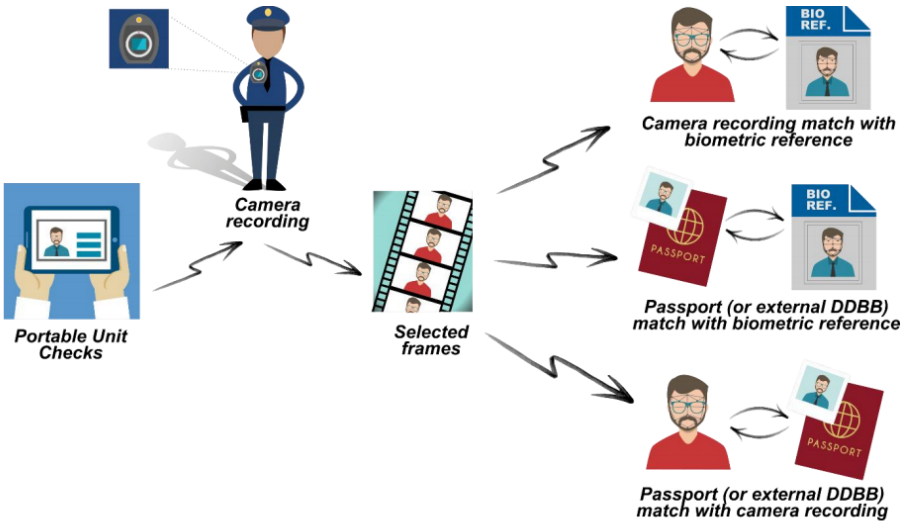

Fig. 3: FMT in the border crossing point [6]

5 Critical Analysis of the iBorderCtrl System

Since the end of the project testing phase in August 2019, the results of the project are yet to be released at the time of writing. That is why the iBorderderCtrl is still considered as experimental and does not prevent anyone from entering the European Union for now. However, the shortcomings of this system are too large to be applied in the future. This section provides a critical analysis of the system and outlines its gaps.

The most widely recognized and used technology for determining the veracity of a person's statements is a polygraph known as „a lie detector". The changes in heart rate and blood pressure, the electrical properties of the skin, and respiratory are classically measured by a skilled polygraph examiner during the polygraph testing. Nevertheless, this process is too expensive, obtrusive, and bad scalable to a large number of interactions. Despite current progress in the development of deception detection systems based on artificial intelligence that permits deception detection to be automated, unobtrusive, and easily used on many people, the iBorderCtrl artificial intelligence facial recognition system is still not sufficiently reliable and is even biased against minorities.

Traditional polygraph interviews are difficult even for experienced polygraph examiners or skilled criminal examiners who conduct time-consuming multiphasic interviews depending on the aim of investigating and the subject. The American Polygraph Association says their accuracy rate above 90 percent when done properly. The artificial lie detector assumes a strong potential for use based just on a set of 16 questions asked by avatars in border control interviews. A person judged to have tried to deceive the system is categorized as high risk or medium risk, dependent on the number of questions considered as falsely answered and on the gained overall risk score with a maximum score of 100. Several reporters and journalists have already tried to test the system. Although they provided honest responses to all questions, they were deemed to be a liar by the machine. The iBoderCtrl team presumed that the system can reach a success rate of 85%, unfortunately, it has only a success rate of 75% for now. But there is still a big space for an error in both cases.

According to the National Academy of Sciences (2003), various techniques have been developed for detecting deception and some of them have potential but none of them does not substitute the polygraph in the near time because its evidence on accuracy is minimal compared to a long-term polygraph investigation.

As previously mentioned, the iBorderCtrl system also might discriminate against people on the basis of their ethnic origin because researchers trained their artificial intelligence on a small sample of mostly European men, so the system has had a higher accuracy rate for that group from the start. For the future real application, research would need to use more diverse study samples, or its accuracy rates will drop for racial reasons. There is also the question, how will mixed-racial group subjects be identified and judged by artificial intelligence? Will they specify their race, or will they automatically detect and judge based on an attributed racial classification?

It is not only ethnic origin which might affect the measures on which iBorderCtrl's deception detection system relies. There are also a lot of people with a range of nervous system abnormalities and correlated differences in social behaviour that might be subject to bias:

- Various types of personality disorders, e.g., attention-deficit and hyperactivity disorder or post-traumatic stress disorder.

- Highly sensitive personality.
- People with depression state or chronic pain conditions, etc.

After the completion of the pilot phase of the iBorderCtrl in Greece, Hungary, and Latvia, the EU wants to implement the system continent-wide. For this, it needs to establish an extensive biometric database called Common Identity Repository. Since August 2019, everyone who crossed the borders of a member state for the first time has been already registered into the new database. It threatens the people's right to privacy because, for people who maintain a social media profile using their real name, it means they have already provided their privacy data for the purpose of the iBorderCtrl.

But there is much more what could be endangered. Even the freedom of thought would be threatened with this technology. If this system can look inside people's minds, it is legal to set it as mandatory for people? Is it in line with human rights? That is a good question which should be solved by the law in the future. For sure, new neurotechnology applications will require new legal frameworks to defend the old human rights including cognitive liberty, the right to mental privacy, the right to mental integrity, and the right to psychological continuity.

6 Conclusion

Despite being considered as controversial, lie detectors have been adopted as an addition to airport security. One such case is the Intelligent Portable Control System, an artificial intelligence-based lie detection technology, which allows faster border crossing processes of EU for third-country nationals. The main purpose of this research was to analyse this innovative system. To achieve this aim, firstly the two-stage procedure and the subsystems of the iBorderCtrl System had to be described, concretely the automated real-time deception detection system, the biometrics tools (fingerprints and palm vein tools), the travel document authenticity analytics tool, the face-matching tool, and the hidden human and vehicle detection tool. Then, a critical analysis of the system could be performed. It should be noted that the iBorderCtrl project has a lot of limitations but despite flaws, the technology may still have a lot to offer. Therefore, future research should be focused on suggestions for its improvement.

7 Acknowledgment

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.

References

[1] Holmes, M. Latham, A. Crockett, K, O'Shea, J. Near real-time comprehension classification with artificial neural networks: decoding e-Learner non-verbal behaviour, IEEE Transactions on Learning Technologies, Year: 2017, Volume: PP, Issue: 99, DOI: 10.1109/TLT.2017.2754497.

[2] Rothwell, Janet & Bandar, Zuhair & O'Shea, James & McLean, David. (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.

[3] Crockett, Keeley, Athos Antoniades, Wasiq Khan & Georgios Emmanouil Boultadakis (2018). Intelligent Deception Detection through Machine Based Interviewing, Available from: https://www.researchgate.net/publication/328399576_Intelligent_Deception_Detection_through_Machine_Based_Interviewing Accessed: 2020-10-30

[4] 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: 2020-10-30

[5] What is iBorderCtrl? IborderCtrl.no (2019). Available from: https://iborderctrl.no/start Accessed: 2020-10-30

[6] Rodríguez Carlos-Roca, Laura; Isabelle Hupont Torres & Carles Fernandez Tena (2018). Facial recognition application for border control, Available from: https://www.researchgate.net/publication/328399474_Facial_recognition_application_for_border_control Accessed: 2020-10-30