Adapted Psychological Profiling Verses the Right to an Explainable Decision

Keeley Crockett[1], Jonathan Stoklas[2], James O'Shea[1], Tina Krügel[2], Wasiq Khan[1]
[1]*School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University,UK,*
[2]*Institute for Legal Informatics, Leibniz Universität Hannove, Hannover, Germany*
{k.crockett,j.d.oshea, w.khan}@mmu.ac.uk, jonathan.stoklas, kruegel @ iri.uni-hannover.de}

Keywords: Psychological Profiling, Artificial Neural Networks, Decision Trees, GDPR

Abstract: Adaptive Psychological Profiling is the process of determining a person's internal mental state through the analysis of a person's non-verbal behaviour. Silent Talker is a pioneering psychological profiling system which was developed by experts in behavioural neuroscience and computational intelligence. Designed for use in natural conversation, Silent Talker combines image processing and artificial intelligence to classify multiple visible non-verbal signals of the face during verbal communication to produce an accurate and comprehensive time-based profile of a subject's psychological state. Silent Talker uses a unique configuration of artificial neural networks, hence, it is difficult to understand how the classification of a person's behaviour is obtained. New legislation in the form of GDPR, now requires individuals whom are automatically profiled, to have the right to an explanation of how the "machine" reached its decision and receive meaningful information on the logic involved. This is difficult in practice, both from a technical and legal point of view. This paper, uses an application of psychological profiling within a pilot system known as iBorderCtrl, which detects deception through an avatar border guard interview during a travellers pre-registration to demonstrate the challenges faced in trying to obtain explainable decisions from models derived through Computational Intelligence techniques.

1 INTRODUCTION

Psychological Profiling is a technique most well known as a tool used within criminal investigations utilising methodologies from both law enforcement and psychology (Bonn, 2017). It involves the detailed and intricate analyses of the non-verbal behaviour of a person, often in an interview situation to detect their mental state. The expertise and training required by a human to undertake this kind of profiling is complex – requiring simultaneous conjecture of many non-verbal signals. Adaptive psychological profiling utilises computational intelligence techniques to build models of non-verbal behaviour for different mental states, i.e. deceptive behaviour or more recently to detect comprehension levels in education. For example, Silent Talker (2018), a profiling system for lie detection uses hierarchies of neural networks to module deceptive behaviour. However, neural networks are by nature 'black boxes' where it is difficult to understand how the trained networks determine if a person is deceiving or not.

The European data protection reform package that came into force in May 2018 consists of the General Data Protection Regulation (Regulation 679/2016/EU, "GDPR") and the "law enforcement directive (680/2016/EU). The GDPR potentially has a worldwide impact on business models and research activities carried out within industry and academic institutions that utilise computational intelligence (CI) algorithms. Specifically, it states the rights of an individual not to be subject to automated decision-making, such as profiling, unless explicit consent is given. In addition, in any aspect of automated decision making, the individual has the right to either opt out or be provided with an explanation of how the automated decision was reached. This would be achieved through disclosure of "the logic involved" (article 13 (GDPR, 2016). When profiling, the data controller should use appropriate mathematical and statistical procedures and that data should be accurate (free from bias) in order to minimize the risk of errors.

This legislation presents many challenges when using CI for modelling complex problems that involve people. How do we provide an explainable

decision suitable for all stakeholders when using 'black box' CI algorithms? The stakeholders are the experts who designed, validated and tested the system, the business or customer who commission the system and the member of the public who receives the automated decision from the system. This paper explores this issue using an application of an automated deception detection system utilised within a pilot system known as iBorderCtrl, which detects deception through an avatar border guard interview during a travellers pre-registration. The finial l neural network classifiers are replaced with traditional decision trees to provide a set of rules on how decisions about deceptive behaviour are reached. The complexity and size of the rule sets produced show that whilst an expert, may have some understanding of the rules, it would be extremely difficult for a member of the public to understand and the expert could not be able to say precisely why these particular rules were derived or explain what they mean.

Section 2 of this paper defines what is meant by psychological profiling in the context of this work, whilst Section 3 explains the legal perspective of some aspects of automated decision making in light of the GDPR. The case study of profiling EU travellers is described in Section 4 and used to illustrate the challenges of developing explainable profiling systems. Section 5 provides the methodology used to conduct empirical experiments on a deception detection profiling system and presents results using both neural networks and decision trees in terms of explainability. Finally, section 6 provides some important considerations for both the legal and computational intelligence communities.

2 PSYCHOLOGICAL PROFILING OVERVIEW

Adaptive Psychological Profiling is the process of determining a person's internal mental state (beliefs, desires, and intentions) through analysing their external behaviour by means of Computational Intelligence (CI) based components. Furthermore, it is based on a generic architecture which is adapted to different application domains and optimised through a process of machine learning. The first such architecture is known as "Silent Talker" (ST) (Bandar et al., 2004). ST uses complex interactions between non-verbal features in a moving video feed from an interviewee to classify truthful or deceptive behaviour. The ST architecture has been adapted for different internal mental states. One such adaptation is for comprehension in intelligent tutoring in the classroom (Holmes et al 2018). Another ethnic / cultural adaptation extended comprehension classification to Tanzanian women for informed consent in a clinical trial (Buckingham et al, 2014). Other ongoing work includes an avatar based deception detection interview integrated into a smart border crossing system (Crockett et al, 2017). The case study used in this paper focuses on the complex problem of the psychological profiling of liars – the next section looks more deeply into the science of lying and why this in particular a challenging problem for computational intelligence in terms of building a model and in trying to explain automated decision making.

2.1 The Science of Lying

There are various different types of lie, with different contextual motivations and different ways of classifying them. For example Ganis et al. (2003) used two classes, whether the lies fit into a coherent story and whether they were previously memorized. Alternatively, Feldman et al. (2002) presented a taxonomy of lies with 10 coding's, for lies produced by participants with 3 different self-presentational goals. Regardless of context, there is a general psychological principle that the act of deceiving produces changes in behaviour has a long history dating back to the Hindu Dharmasastra of Gautama, (900 – 600 BC) and the philosopher Diogenes (412 – 323 BC) according to Trovillo (1939).

There are a number of factors, proposed by psychologists which may be influential drivers of behavioural change during deception. These are general arousal / stress, cognitive load, behaviour control and special cases of arousal, guilty knowledge and duping delight. Stress is the oldest driver to be measured for lie detection. Following work by Angelo Mosso in the late 19th and early 20th centuries using pulse and blood pressure, the polygraph was invented by Larson in 1921 (International League of Polygraph Examiners, 2016). The Cognitive Load driver derives from the work of George A. Miller (1956), whose Magical Number 7 (+/- 2) indicated that there were a limited number of "mental variables" that an individual could process concurrently. Therefore, someone trying to construct and remain consistent with a false account would be under increased cognitive load. Behaviour control occurs when deceptive interviewees deliberately try to control themselves in order to make an honest and convincing impression. It is postulated that attempts to control behaviour will increase in higher-stakes scenarios (Caso et al., 2005). Guilty knowledge (Concealed Knowledge) is a test of whether a suspect has information related to a crime that an innocent

person would not possess. When exposed to such information an interviewee is expected to produce a reaction detected by instrumentation (MacLaren et al., 2001). Duping delight is believed to occur in an interview when the deceiver experiences pleasurable excitement at the prospect of successfully deceiving the interviewer, particularly in the presence of observers (Sen et al., 2018).

2.2. Automated Lie Detection

The field of computational intelligence provides a wealth of algorithms which are suitable to build models of liars automatically. Silent Talker (ST) (Silent Talker, 2018) differs from many other lie detectors in its assumption that deceptive non-verbal behaviour is the outcome of a combination of psychological drivers and that it cannot be characterized by a simple, single indicator. ST uses complex interactions between multiple channels of microgestures over time to determine whether the behaviour is truthful or deceptive. A microgesture is a very fine-grained non-verbal gesture, such as the right-eye moving from half-open to closed. This can combine with other microgestures from the right eye to detect a wink or both eyes to detect a blink. Measured over time these can combine to measure blink rate. Complex combinations and interactions of typically 38 channels and interactions between them can be compiled into a long vector, over a time slot, which can be used to classify behaviour as truthful or deceptive over the slot. Microgestures are significantly different from micro expressions (proposed in other systems), because they much more fine-grained and require no functional psychological model of why the behaviour has taken place. Furthermore, because there are so many channels contributing to the analysis, behaviour control is infeasible. Typically, using a recording device such as a web cam, salient features (e.g. eye half) are identified in an individual video frame by a layer of object locators. The states of the objects are detected by the pattern detectors (e.g. eye half open). The channel coders complied the outputs of the pattern detectors over time (e.g. sequence of eye movement indicating a blink) and the deception classifier uses this long vector compiled by the channel coders. The ST approach to lie detection is based on a “black box” model, the conjecture that these and other (unknown) factors act as drivers of non-verbal behaviour, resulting in distinctive features that can be used to discriminate between deceivers and truth-tellers. Silent Talker is in itself an automated profiling system and is being piloted as basis for an automated deception detection system to profile travellers crossing European borders at a pre-registration phase and we will be described in section 4 of this paper.

3 THE GDPR

3.1 Automated decision-making under the GDPR

From a legal perspective, various issues arise. In 2016, the European Union agreed on a data protection reform package including the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679, 2016), which went into force on 25 May 2018. The GDPR introduces various new regulations which affect both profiling and the use of computational intelligence-based systems. As explained above, profiling and automated decision-making are both covered by art. 22 GDPR. According to art 22 (1) GDPR, an automated decision is a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. One of the most obvious challenges in this regard is the fact that almost any decision in an increasingly digitized world might have at least a mediate legal effect as well (Von Lewinski, 2018). Therefore, the interpretation of this requirement should be rather restrictive, whereas any single case shall be assessed based on objective factors (Martini, 2018a). While this result seems to be sound and necessary, persons without a legal background might face difficulties in assessing whether their decision is to be seen as automated decision-making or not. In particular, decisions which do not produce any legal or other similarly significant effects are not subject to art. 22 GDPR. An automated lie detection system, however, will most probably always cause significant effects on the persons, both from possible use-cases, as well as with regard to personality rights (e.g. reputation).

3.2 Safeguards and information obligations

For decisions falling within the scope of art. 22 GDPR, certain safeguards need to be considered. According to art. 22 (3) GDPR, the data controller shall *implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*. While these requirements could be easily implemented from both an organisational and technical point of view, additional obligations can be

found in the data subject's rights: According to art. 13 (2) lit. f), 14 (2) lit. g) and 15 (1) lit. h) GDPR, the data controller is required to inform the data subject about

- the existence of automated decision-making as referred to in art. 22,
- meaningful information about the logic involved, and
- the significance and the envisaged consequences of such processing for the data subject.
- In addition, information has to be provided in concise, transparent, intelligible and easily accessible form, Art. 12 (1) GDPR. This also applies to information obligations regarding automated decision-making (Martini, 2018b).

These regulations, however, are not sufficiently clear from a legal point of view (Bräutigam & Schmidt-Wudy, 2015). While it shouldn't be a practical problem to inform about the existence of automated decision-making, it remains unclear what is meant with "meaningful information on the logic involved". Also, the criteria for assessing whether information provided complies with the requirements imposed by art. 12 (1) GDPR, meaning that they should be in intelligible form, are unclear.

3.3 Meaningful information on the logic involved

Providing meaningful information can be challenging in practice. In particular, algorithms used for automated decision-making might be at the same time crucial for certain business models. Therefore, revealing the whole algorithm would interfere with the legitimate interest of companies to protect their trade secrets. In that regard, the German Constitutional Court ruled in 2014 that the "Schufa", a credit scoring institute, was not obliged to reveal their algorithm as it was at the same time a trade secret (German Constitutional Court, 2014). According to the ruling, only the personal information which had been considered for a scoring decision should be subject to the information obligations. However, it has to be noted that this decision does not reflect the GDPR, but the German national data protection act which was based on the former data protection directive 95/46/EC. However, protecting algorithms also for trade secrets remains a crucial interest of many companies offering services in a digital society. Therefore, the GDPR shall be interpreted in a way which would not impose such an obligation either (Roßnagel et al. 2015). In particular, recital 63 states that the right to access should not adversely affect the rights or freedoms of others, including trade secrets and intellectual property rights. Therefore, providing information on the basic functioning of an algorithm appears to be sufficient to comply with the obligation to provide meaningful information (Paal & Henneman, 2018). Even though the answer to this question might be subject to upcoming jurisdiction (Schmidt-Wudy, 2018a).

However, technical phenomena like the "black box" often associated with neural network type systems and deep learning would impose additional challenges for this requirement. Self-learning algorithms might adjust their functioning and resolving how they actually behave might be difficult. In addition, information would need to be updated frequently, based on the algorithm's adjustments. While it would be at least possible to provide information on how the algorithm learns, it might be questionable in how far this would be to provide sufficient information necessary to ensure a fair and transparent processing (see recital 60). Consequently, a proper solution for this issue remains unclear.

3.4 Intelligible information for the data subject

Another legal issue with regard to the information obligations is the requirement to provide intelligible information. This leaves room for certain interpretation: Should the information be intelligible for the data controller, for the individual data subject, or rather for an objective, reasonable and informed third party? (Schmidt-Wudy, 2018b). In that regard, it needs to be considered that data controllers might have a substantial advantage both in knowledge of their systems and technology in general. While detailed technical information could be on the one hand seen as a maximum level of transparency, an average data subject will most probably not be able to understand such information. Therefore, information should be less detailed than it would be theoretically possible if this ensures that the data subject can actually understand the information. This is also reflected in art. 12 and recital 58, stating that the data subject shall be addressed using clear and plain language. Last but not least, another challenge is the fact that data subjects can have very different background-knowledge helping them to understand information. People who frequently use ICT services might be more familiar with the functioning of algorithms than people who can barely use a computer. If the GDPR is required to ensure that every *individual* data subject understands the logic involved, data controllers would have no legal certainty as to whether they comply with the legal

requirements or not. Therefore, the information provided to describe the logic involved should be intelligible for an objective, reasonable and informed third party persons ("the average user"), while at the same time providing as much information as possible.

3.5 Challenges for the technical community

As outlined above, many issues regarding automated decision-making derive from legal problems. However, there are certain issues which also require input and solutions from the technical community, in particular:

- How to properly assess the legal situation regarding automated decision-making and on how to apply proper safeguards?
- How to explain an algorithm without leaking trade secrets?
- How can algorithms based on computational intelligence be explained?
- Can the information on how an algorithm learns be sufficient to understand it's functioning and decision-making?
- Can self-learning algorithms also explain their decision-making, and could this be updated frequently for every user?

4 CASE STUDY: PROFILING TRAVELLERS ACROSS SCHENGEN BORDERS

iBorderCtrl, short for, Intelligent Portable ContROl SyStem is a three year H2020 project, funded by the European Union, which is currently developing novel mobility concepts for land border security. The system will enable authorities to achieve higher throughput at the crossing points whilst guaranteeing high security level through faster processing of passengers within vehicles or pedestrians, whilst targeting criminal activities such as human trafficking, smuggling and terrorism. In addition, the system will aim to reduce the subjective control and workload of human border agents and to increase the objective control through non-invasive automated technologies. Through travellers engaging in a pre-registration step, the aim is to ensure they have a speedier border crossing. (Crockett et al., 2017). A full description of the project can be found here http://www.icross-project.eu/ iBorderCtrl features a unique combination of state-of-the-art biometric tools which will provide risk scores to a Risk Based Assessment Tool (RBAT) that will act as an automated decision-maker on the status of the traveller as they arrive at the border crossing point (Green is proceed, Amber is second line check and Red is refusal). It is important to say that iBorderCtrl is a human in the loop system and therefore provides advice to human border guards who ultimately have the final say. The focus in this paper is on the profiling of travellers deceptive behaviour in the pre-registration step using a physcholigical profiling system called ADDS (Automated Deception Detection system) (O'Shea et al, 2018) and how such a system when deployed in the field, provides numerous challenges if asked to provide an explainable decision to different stakeholders: the research and development team of ADDS, the Border Guards and their managers and the travellers using the system. The next section provides a brief overview of ADDS.

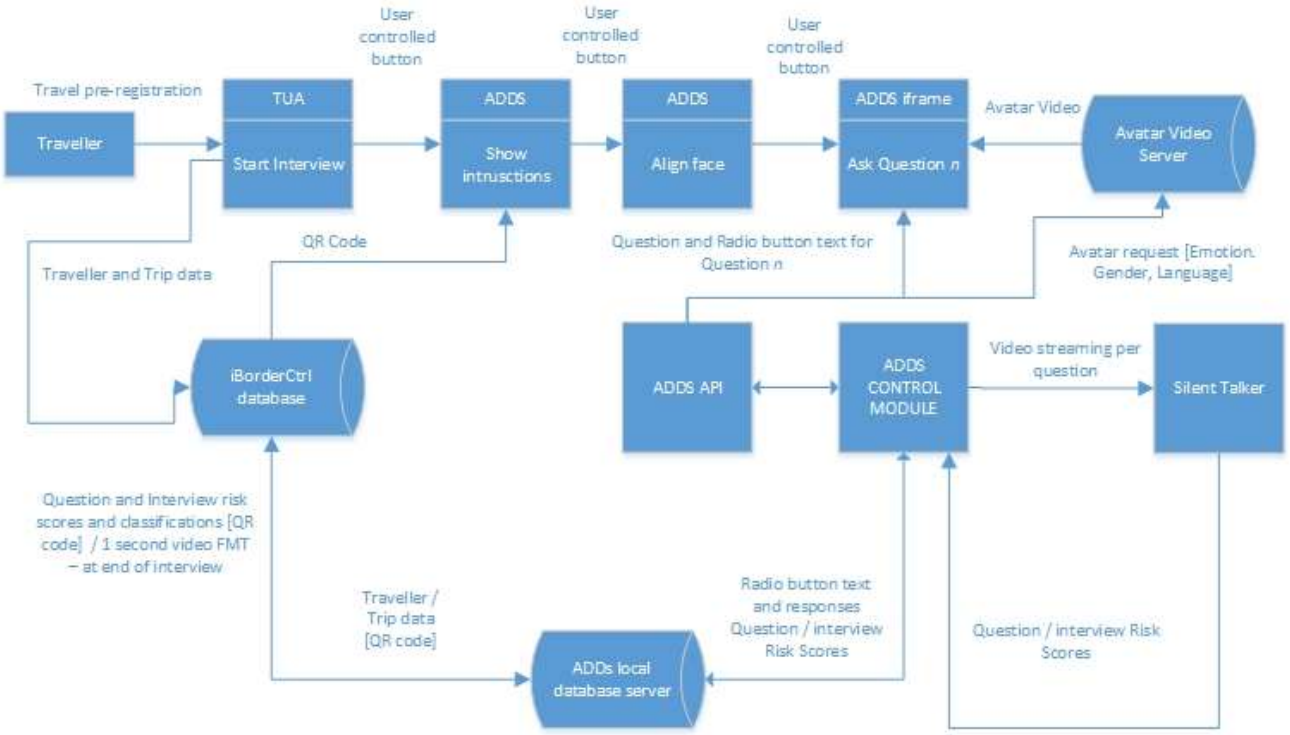

Figure 1: ADDS Dataflow.

4.1 Automated Deception Detection system

In the pre-registration phase, each traveller after entering the information about their trip will be required to be interviewed by a Border Guard avatar. Information is exchanged between the iBorderCtrl System and the ADDS system using a unique QR code which is generated per traveller trip. An overview of the ADDS dataflow can be found in figure 1. In the pilot studies, consenting adults who meet the ethical criteria will be asked 16 questions, similar to those asked at border crossing points. The interview will last less than 2.5 minutes. ADDS will be responsible for conducting the interview where the Avatar asks questions, utilising three attitudes (puzzled, neutral and positive) and two avatars, one male and one female which are randomly assigned. An example of a Border Guard avatar (designed by Stremble) is shown in Figure 2.

Figure 2: Female Avatar Border Guard.

The non-verbal behaviour of each video question response will be analysed by the Silent Talker system (O'Shea et al, 2018a) which will output, for each question, the deceptive risk score. In ADDS, 38 non-verbal facial channels are utilized which vary in complexity. Each channel is coded to the bipolar measurement range [-1, 1] by the Channel Accumulator (O'Shea et al, 2018a) and ultimately are then grouped into channel vectors based upon a time slot (i.e. 1 to 3 seconds) before being encoded within the image vector. Figure 3, shows an example of the back end processing carried out by the Silent Talker component of ADDS. The bottom screen, displays the live video stream for a specific interview question,

whilst on the right the number of truthful, deceptive and unknown slots are shown. At the conclusion of the interview, questions and interview risk scores and their associated classifications, along with one second worth of video frames are uploaded to the iBorderCtrl database to be used by Face Matching Module (Rodiguez et al. 2018) and RBAT (Crockett et. al. 2017).

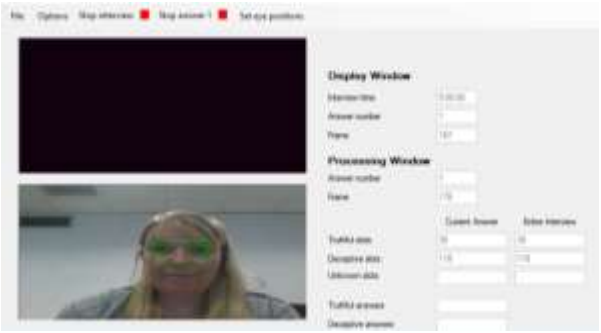

Figure 3: Backend Silent Talker Processing.

5 METHODLOGY

An empirical study was conducted using 30 participants whose non-verbal behaviour was recorded whilst engaged in an online interview with a static border guard avatar (O'Shea et al., 2018a). The aim of the experiment was to derive models of truthful and deceptive non-verbal behaviour using both hierarchical neural networks and decision trees to classify deception and truthfulness. The hypothesis tested was:

H0: A decision made by an automated deception profiling system can be explained using decision tree models

H1: A decision made by an automated deception profiling system cannot be explained using decision tree models

After ethically consenting to take part in the study, the 30 participants took part in a role play exercise which involved packing a suitcase with 6 items typically taken on a holiday. Each participant was randomly assigned either a truthful or one of four deceptive scenarios designed to cover high and low stakes deception. For example, based on the literature, it was anticipated that a person being deceptive about packing some illegal agricultural produce would generate higher arousal levels than a person transporting drugs. Following the role play, participants were then interviewed by a border guard avatar and were asked 13 questions which are typical of those asked by border guards. Full details of the experimental methodology are described in (O'Shea, 2018). Following data preparation (described in section 2.1), two classification models were developed. One based on the hierarchal ANN model used by Silent Talker and the other using infamous Quinlan's C4.5 decision tree (Quinlan, 1994).

5.1 Data

From the image data of the 32 participants, 86584 image vectors were collected where each vector contained the states of each of the 38 non-verbal channels. Ground truth was established for each participants interview question through knowledge of the scenario that they role played. I.e. truthful (43051 image vectors) or deceptive (43535 image vectors). Out of the 32 participants, there were 17 deceptive and 15 truthful interviews, 22 males and 10 females with a mix of ethnicities. In ADDs, the final ANN classifies truthfulness or deceptiveness is based upon an activation level in the range [-1, 1] which was determined from the data set. The deception risk score, *Dq*, of each of the 13 questions was defined as

$$D_q = \frac{\sum_{s=1}^{n} d_s}{n} \qquad (1)$$

Where d_s is the deception score of slot *s* and *n* is the total number of slots for the current question. In order to obtain a classification for each vector, the following thresholds were applied (O'Shea et, a. 2018a).

IF Question_risk (D_q*) <= x THEN*
Image vector class = truthful
ELSE IF Question_risk (D_q*) >= y THEN*
Image vector class = deceptive
ELSE
Indicates not classified
END IF

Where x = -0.05 and y = +0.05 []. Thus if a question risk score was within this range, a classification could not be allocated.

5.2 Results and Analysis

In (O'Shea et al, 2018a), two methods for training, validation and testing were reported: *n-fold* cross validation and leave pair out. The latter being more of

an appropriate measurement of accuracy for unseen participants, which is required when a system such as ADDS is deployed in the field. However, for the purposes of this paper, in the context of comparing models in terms of classification accuracy and their ability to produce an explainable decisions, cross validation is used as initial work showed there was little difference in induced decision tree size. With no ANN or C4.5 optimisation, the best tree from performing *10-fold* cross validation contained 1072 rules. Table 1 shows the overall classification accuracy of 10-fold cross validation for both the ANN (ADDS-ANN) and C4.5 (ADDS-DT)

Table 1: 10-fold cross validation results

Method	%Train AVG	%Test AVG	%Class-Accuracy
ADDS-ANN	97.03	96.66	96.8
ADDS-DT	98.9	98.8	98.8

5.2.1 Are Decisions Explainable?

Figure 4 shows a snapshot of the best decision tree which contains 1072 rules.

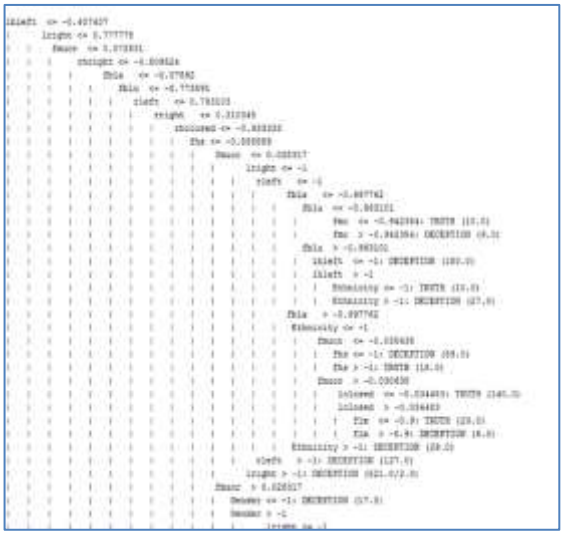

Figure 4: Rule Snapshot

The rules induced from the dataset represent patterns of non-verbal behaviour for specified channels, when combined together allow the classification of deception verses truth for a given risk score. One rule from this tree which gives a classification of deception can be extracted as follows:

IF lhleft < -0.407407 AND lright <= 0.777778 AND fmuor <=0.072831 AND rhright <= 0.310345 AND rhclosed <=-0.93333 AND fhs <= -0.888889 AND fmour <=0.028317 and lright <=-1 and rleft <=-1 and fbla <=-0.997762 and fblu <=-0.963101 and fmc > -0.942354 THEN CLASS DECEPTION.

Analysing this rule, as experts, we see information on four non-verbal channels associated with the eyes: left eye looking left (lleft), left eye looking right (lright), right eye half closed (rhclosed), right eye looking left (rleft) and 5 channels containing information about the state of the face including the horizontal movement of the face (fhs) face angular movement up-on-right (fmuor) and the degree of blushing/blanching (fblu). Face channels track face the movement along the X-axis and Y-axis using the coordinates and dimensions of the face found by the Face Object Locator ANN (Buckingham et al, 2012). Likewise, the state of each eye channel is determined from a Pattern Detector ANN (O'Shea et al, 2018) observing the left/right eye image and/or from the application of logical decision(s). The values for each channel are determined empirically by the pattern detector ANNS and the channel encoder ANNS in the bipolar range [1 and -1].

In this application, the rules are complex and look at combinations of fine grained non-verbal behaviour i.e. movement of facial features. Due to this complexity, individual rules are difficult for an average human to comprehend. They could not for example be replicated by a human. As the problem is complex the tree is large – previous work (O'Shea et al, 2018b) suggests pruning may lead up to a 25% reduction in rules. A sacrifice in classification accuracy occurs but still the quantity of rules is large and difficult to comprehend. But is this problem scenario based? If automated profiling was applied to a simpler more typical problem, such as a bank loan or mortgage application then perhaps the learnt rules could be understand by all stakeholders – the expert, the member of the public and the bank manager. Consider for example, a small dataset containing 434 instances for applications for personal loans. 238 instances are reject samples and 196 accept. The dataset contains just 14 attributes. Using C4.5 and *10-fold* cross validation, a classification accuracy of 74.8% is achieved and the best tree contained 27 rules. A sample rule is shown below:

IF TimeAtBank(years) <=2 AND
TimeEmployed(years) < 1 AND

ResidentStatus = "Rented" THEN Outcome = REJECT LOAN.

A person, profiled by this system, could have the decision explained to them using this rule by a staff member at the bank i.e. they had not been a customer at the bank for long enough and had not been in employment for over a year and they currently lived in rented accommodation. What the staff could not do is explain and show the statistics behind the decision, nor guarantee that there was any bias in the training data that led to the model. Therefore, neither the hypothesis H0 nor H1 can truly be accepted as explainability is determined by problem representation and complexity.

6 CONCLUSIONS

This paper has used a case study of adaptive psychological profiling to examine the challenges of how to produce explainable decisions of CI models to all stakeholders. There are many challenges for both the computational intelligence and the legal communities. Therefore, finding solutions which reflect technical realities while at the same time providing sufficient privacy safeguards will be crucial. This, however, requires a close collaboration of both the legal and technical community, which currently happens very rarely. A closer collaboration between both communities would allow better guidance, such as common guidelines for software developers, standardized frameworks which comply with the GDPR by default, and many more. Therefore, receiving answers to the questions raised in section 3.5 would be an important first step to further deepen the common understanding of technical and legal challenges relating to the GDPR and to foster a debate on the proper interpretation of the GDPR among the legal community, as well as information on how the technical community could be supported in their efforts to comply with legal requirements.

ACKNOWLEDGEMENTS

The iBorderCtrl project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626. Silent Talker research has been supported by Silent Talker Ltd.

REFERENCES

Bandar, Z. Rothwell, J. McLean, D. O'Shea, D, 2004. Analysis of the behaviour of a subject, Publication date 2004/5/3, Patent office US, Application number 10475922

Buckingham, F. Crockett, K. Bandar, Z. O'Shea, J. MacQueen, K. Chen, M. 2012. Measuring Human Comprehension from Nonverbal Behaviour using Artificial Neural Networks, Proceedings, *In Proceedings of IEEE World Congress on Computational Intelligence* Australia, pp368-375, DOI: 10.1109/IJCNN.2012.6252414

Bonn, S. 2017. Criminal Profiling: The Original Mind Hunters, Profiling killers dates back to Jack the Ripper, *In psychology Today*, [online] https://www.psychologytoday.com/us/blog/wicked-deeds/201712/criminal-profiling-the-original-mind-hunters [Accessed 27/7/2018]

Bräutigam/Schmidt-Wudy, (2015) Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung, CR 2015, 56 (62).

Caso, L., Gnisci, A., Vrij, A. and Mann, S., 2005. Processes underlying deception: an empirical analysis of truth and lies when manipulating the stakes. *In Journal of Investigative Psychology and Offender Profiling*, 2(3), pp.195-202.

Civin, D. 2018. Explainable AI could reduce the impact of biased algorithms, [online] https://venturebeat.com/2018/05/21/explainable-ai-could-reduce-the-impact-of-biased-algorithms/ [Accessed 25/07/2018]

Crockett, KA and O'shea, J and Szekely, Z and Malamou, A and Boultadakis, G and Zoltan, S, 2017. Do Europe's borders need multi-faceted biometric protection? *In Biometric Technology Today*, (7). pp. 5-8. ISSN 0969-4765.

Crockett, K. Goltz, S. Garratt, M. 2018. GDPR Impact on Computational Intelligence Research, *In Proceedings of IEEE International Joint conference on Artificial Neural Networks (IJCNN)*, July 2018, in press.

European Parliament. 2016. S*mart Borders: EU Entry/Exit System. Brussels: European Parliament.*

Feldman, R.S., Forrest, J.A. and Happ, B.R., 2002. Self-presentation and verbal deception: Do self-presenters lie more?. *In Basic and Applied Social Psychology*, 24(2), pp.163-170.

Ganis, G., Kosslyn, S.M., Stose, S., Thompson, W.L. and Yurgelun-Todd, D.A., 2003. Neural correlates of different types of deception: an fMRI investigation. Cerebral cortex, 13(8), pp.830-836.

GDPR Portal, 2018, [online]. Available at: https://www.eugdpr.org/ Accessed [27/07/2018].

German Constitutional Court (BGH), 2014. Decision of 28.1.2014 - VI ZR 156/13, [online] https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1. [Accessed 27/07/2018]

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

iBorderCtrl Intelligent Portable Control System [online], Available at http://www.iborderctrl.eu/ [Accessed 12/1/2018].

International League of Polygraph Examiners. 2016.), *Polygraph/Lie Detector FAQs.* [online] http://www.theilpe.com/faq_eng.html. [Accessed 28/7/2018]

Martini, 2018a. *In Paal/Pauly DS-GVO Art. 22*, Fn. 25-28. [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018]

Martini,2018b. *In Paal/Pauly DS-GVO* Art. 22, Fn. 41a. [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018]

MacLaren, V. 2001. A quantitative review of the Guilty Knowledge Test. *In Journal of Applied Psychology*, Vol 86(4), Aug 2001, pp. 674-683

Miller, G. The magical number seven, plus or minus two: Some limits on our capacity for processing information 63 (2), 81-97, (1956).

O'Shea, J. Crockett, K. Khan, Kindynis, P. Antoniades, A. Intelligent Deception Detection through Machine Based Interviewing, *In Proceedings of IEEE International Joint conference on Artificial Neural Networks (IJCNN)*, July 2018, *in press*.

O'Shea, J. Crockett, K. Khan, W. (2018) A hybrid model combining neural networks and decision tree for comprehension detection, *In Proceedings of IEEE International Joint conference on Artificial Neural Networks (IJCNN)*, July 2018, *in press*.

Quinlan, R. 1994. C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers. ISBN 1-55860-238-0.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Rodiguez, L. Hupoint, I. 2018. Facial Recognition Application For Border Control, *In Proceedings of IEEE International Joint conference on Artificial Neural Networks (IJCNN)*, July 2018, *in press*.

Roßnagel/Nebel/Richter, 2015. Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO ZD 2015, 455 (458).

Schmidt-Wudy, 2018a. *In BeckOK DatenschutzR DS-GVO Art. 15*, Fn. 78.3. [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018][1]

Schmidt-Wudy, 2018b. *In BeckOK DatenschutzR DS-GVO Art. 15*, Fn. 78. [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018]

Sen, T., Hasan, M.K., Tran, M., Yang, Y. and Hoque, M.E., 2018, May. Say CHEESE: Common Human Emotional Expression Set Encoder and its Application to Analyze Deceptive Communication. In Automatic Face & Gesture Recognition (FG 2018), 2018 13th IEEE International Conference on (pp. 357-364).

Silent Talker Ltd. 2018 [online] https://www.silent-talker.com/. [Accessed 29/07/2018]

Stoklas, J. Krugel, T. Schutze, R. (2018). Legal, ethical and social impact on the use of computational intelligence based systems for land border crossings, *In Proceedings of IEEE International Joint conference on Artificial Neural Networks (IJCNN)*, July 2018, *in press*.

Trovillo, P. 1939. History of Lie Detection, *In Journal of Crim. L. & Criminology*, 848.

Von Lewinski, 2018,. *In BeckOK DatenschutzR DS-GVO Art. 22, Fn. 28.* [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018]

Paal/Henneman, 2018. *In Paal/Pauly DS-GVO Art. 13*, Fn. 31. online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokdatens_24%2Fewg_dsgvo%2Fcont%2Fbeckokdatens.ewg_dsgvo.a28.htm. [Accessed 27/07/2018]