Reading the criminal mind

Exploring novel methods of memory detection

Van der Cruyssen, I.A.

Publication date
2023

1
General introduction

In October 2009, neuroscientist Adrian Owen received a phone call from his postdoctoral researcher Martin Monti. They had done it! They had managed to read Patient 23's mind. Five years earlier, the then 19-year-old Patient 23 had been in a terrible motorcycle accident. He had survived the crash, but had been in a vegetative state ever since. He no longer reacted to anything that happened around him until that particular night in October 2009. The researchers had put the patient in an fMRI scanner and asked him some questions. They had explained to him that when he wanted to answer "yes" he had to think about playing tennis (which would give a spike of activity in his premotor cortex) and when he wanted to answer "no" he had to think about walking around his house (which would activate his parahippocampal gyrus - an area in the temporal lobe). And it worked. After 5 years, the researchers were able to communicate with Patient 23 by reading his mind (Monti et al., 2010; Somers, 2021).

The idea of mind reading has always evoked a pervasive fascination, not only in the academic world but also in popular discussions. The idea has inspired many movies and TV series, including the most popular TV series of the past year, Stranger Things (IMDb[1], 2022). In this series, the main character Eleven could intentionally intrude into people's minds and relive their memories. Although most movies and TV series make this skill look futuristic, the above example of Patient 23 shows that these ideas might no longer be just science fiction. In addition to tapping into the mind of vegetative patients (Monti et al., 2010), it has been shown to be possible to discover what someone is dreaming while they are sleeping by measuring their nerve impulses to muscles with an electromyogram (Oldis, 2017), or to reconstruct movie trailers someone has seen from fMRI signals (Nishimoto et al., 2011). Mind reading has many opportunities and could not only be of interest for people who *can* not talk (e.g.,

[1] IMDb is the world's most popular and authoritative source for news about movies and TV series. Its annual rankings of the most popular movies and TV series is determined by the actual page views of the more than 200 million monthly visitors to IMDb.

because they are in a coma or sleeping), but also for people who do not *want* to talk – such as suspects of a crime who refuse to confess.

Reading the criminal mind

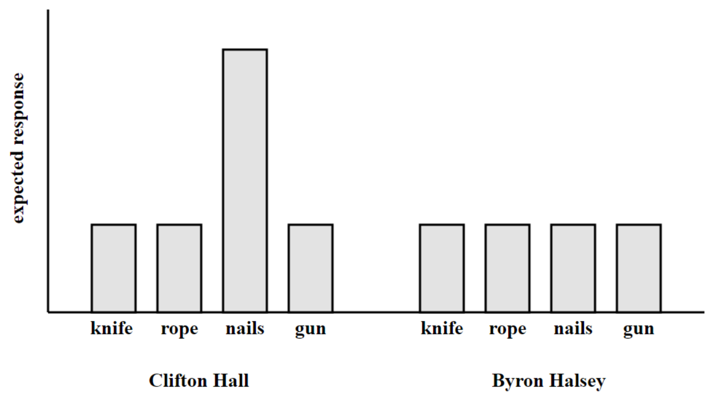
On the night of November 14, 1985, a seven-year-old girl and her eight-year-old brother went missing in New Jersey, United States. The next morning, they were both found dead in the basement of their house. The police immediately arrested Byron Halsey, who was helping to raise the children, and Clifton Hall, the neighbor of the family. Not long after the arrest, Byron Halsey was charged with murdering the two victims. Clifton Hall was released and was later called as an eyewitness in court. After spending 19 years in prison, DNA evidence revealed that not Byron Halsey, but neighbor Clifton Hall was guilty of committing the murders. In the meantime, Clifton Hall had committed three other crimes (Innocence Project, 2019).

All that time, Clifton Hall of course knew what he had done. All the details of the crime had been stored in his memory. To examine whether a suspect of a crime has incriminating crime knowledge, even if they deny it, recognition of crime-related details can be detected using memory detection procedures. For example, if the investigators of the above case could have discovered that Clifton Hall was aware of several facts about the crime that only an actual perpetrator could know (e.g., the location where the bodies were found or the manner of death), while Byron Halsey did not possess any of this knowledge, a miscarriage of justice could have been avoided, and three crimes could possibly have been prevented.

Memory detection (also referred to as Guilty Knowledge Testing or Concealed Information Testing) covers a group of techniques with the same goal and methodology (Lykken, 1959, 1960; Verschuere et al., 2011). The goal is to detect through behavioral and physiological measures whether someone has critical crime knowledge. The typical methodology involves the presentation of critical crime information within a series of similar, crime-unrelated information. If the examinee shows systematically stronger responses to the crime-related items than to the similar, crime-unrelated alternatives, concealed crime knowledge can be inferred. For example, if the investigators in the above example had tested the suspects' awareness of what the murder weapon was, responses to the real murder weapon (nails) could have been compared to several equally plausible murder weapons (e.g., knife, gun, rope…), see Figure 1.

Figure 1

Expected data pattern if a memory detection test would have been used in the Byron Halsey case



After decades of research, it is well-established that memory detection is a valid way for discovering "knowledgeable" individuals (Verschuere et al., 2011). A meta-analysis showed areas under the Receiver Operating Characteristic (ROC) curve well above chance level ranging from .735 to .848[2] (Meijer et al., 2014). Another selling feature of memory detection is that (in contrast to traditional lie detection methods such as the Control Question polygraph Test; Ben-Shakhar, 2002) it is not biased against the innocent (Lykken, 1988). While a guilty suspect responds differently to the crime-related item than to the control items,

[2] The area under the ROC curve is a measure of diagnostic accuracy of a test. It ranges from 0.5 to 1, where a value of 0.5 indicates a chance level accuracy and suggests no discrimination, while a value of 1 reflects a perfectly accurate test (Mandrekar, 2010).

an innocent suspect will not recognize the crime-related item and will therefore respond similarly to all presented items. These findings show the potential of memory detection. As such, the test has become an essential aid in criminal investigations in Japan (Osugi, 2011).

Traditionally, the possession of concealed knowledge is detected based on autonomic nervous system responses: Skin conductance, heart rate, and respiratory responses (Verschuere et al., 2011). Recently, it has been shown that in addition to the traditional measures, also reaction times (Suchotzki et al., 2017; Verschuere et al., 2014), the P300 component (i.e., a positive event-related potential that occurs after a meaningful piece of information is recognized; Fabiani et al., 1986; Rosenfeld et al., 1991), and fMRI (Langleben et al., 2002) can be used to detect concealed information. With these more recent measurements, accuracy rates rivaling those of the traditional measures can be obtained (Meijer et al., 2016). In the last decade, there is also renewed interest in eye movement measures for detecting concealed knowledge (Lancry-Dayan et al., 2022), especially since eye movements occur rapidly, uncontrollably, and sometimes even in the absence of conscious awareness (Hannula et al., 2010).

Challenges of memory detection

Although memory detection has proven to be a powerful tool for detecting the recognition of crime-related information, it is not without its obstacles. Four main challenges of the forensic application of memory detection include the leakage problem, the risk of countermeasures, item selection difficulty, and the test's limited applicability.

Leakage

One of the main challenges of memory detection is the leakage problem (Bradley et al., 2011). The assumption that only guilty individuals have knowledge about a crime might not always be valid. Innocent suspects may inadvertently acquire information about a crime through various means such as newspapers, social media, or during the interrogation itself. Since the test detects crime knowledge, but not how this knowledge was acquired, leakage significantly increases the risk of false positive results (Bradley et al., 2011). Although in real criminal investigations, an innocent suspect could explain how they acquired this crime knowledge, the leakage problem poses a great challenge for memory detection.

Countermeasures

Another challenge of memory detection is the potential use of countermeasures (Ben-Shakhar, 2011; Peth et al., 2016). Countermeasures refer to techniques guilty suspects can deliberately use to control their responses and avoid detection (i.e., make them look innocent when they are actually guilty). By using either physical countermeasures such as inflicting pain by biting their tongue or mental countermeasures such as focusing on exciting memories, an enhanced response during the control items could be elicited, which can lead to false negative results. A review by Ben-Shakhar (2011) revealed that it is possible and unfortunately even quite easy to enhance responses to control items and bypass memory detection tests.

Item selection

The selection of proper crime-relevant and control items is crucial for a successful implementation of memory detection. Nonetheless, this process can be difficult (Krapohl, 2011). Memory detection tests must use crime-relevant details that are present in the perpetrator's memory. However, deciding which of all possible details of a crime scene are salient to the culprits and remembered by them, can be a challenging task. Especially in complex crime scenes, it can be hard for the investigators to know what the examinee encoded and still remembers days or even weeks after the crime. Furthermore, in what form should the selected item ideally be presented? In a typical memory detection test, items are presented verbally. However, memory research suggests that pictures are better remembered and more easily recognized than their verbal counterparts (Kirkpatrick, 1894).

Limited applicability

Finally, memory detection has a limited applicability as it can only be used in narrowly defined situations. The physiological and neural measures require a laboratory setup and an experienced examiner which can be challenging in settings like airports, border control, or police interviews. With technology constantly evolving (which was further sparked by the COVID-19 pandemic forcing everyone and everything to go online), the possibilities of online methodologies are increasingly being tested (Kees et al., 2017). This includes memory detection research, which may have some significant advantages. No more lab, experienced examiner, and dedicated and expensive hardware would be needed. Large-scale memory detection programs could be implemented at critical borders, where they could identify travelers who require additional questioning (Kleinberg et al., 2019).

The current dissertation

In the past decades, research on memory detection has expanded considerably, and researchers are constantly tinkering with the different methods to develop the best possible form of it. However, some important challenges remain that prevent the test from becoming widely used. In the current dissertation, I am going to take initial steps in examining some new methods that could resolve some of these challenges. To this end, the current PhD consists of four empirical lines of research.

In the second chapter, I addressed the question of whether items are better presented pictorially or verbally in memory detection. Memory research suggests that pictures are better remembered and more easily recognized and recalled than their verbal counterparts (Kirkpatrick, 1894). However, both in practice in Japan as well as in most empirical studies items are presented verbally. I examined which modality is optimal, and tested whether encoding and testing modalities interact in an online memory detection test based on reaction times.

In the third chapter of this dissertation, I explored the promising new development of memory detection based on eye movements. Initial memory detection studies based on eye tracking produced modest detection efficiency rates. Recently, Lancry-Dayan et al. (2018) argued that these initial studies might have been sub-optimal because they used a serial presentation of their items. They introduced a novel approach, applying a combination of both parallel and serial item presentation with a working memory task. This new paradigm resulted in areas under the ROC curve ranging from 0.89 to 0.97 in detecting familiar faces. I adopted this promising new paradigm and tested it in a mock crime setting. Additionally, I examined whether this method might provide a solution for one of the biggest challenges of memory detection: The information leakage problem (e.g., Bradley et al., 2011). Specifically, I examined whether innocents who gained knowledge about the crime by reading about it can still be distinguished from actual guilty suspects.

In the fourth chapter, I examined whether a simple webcam could be used as an eye tracker. One of the major promises of memory detection based on eye movements lies in the possibility of conducting tests remotely and without a laboratory setup. Remote memory detection has several important advantages. It has been argued that it could bypass countermeasures when the examinee is unaware of being tested (Elaad, 2011) and that it has the potential to be used for rapid detection on a large scale (Kleinberg et al., 2019). As a first step in assessing the potential of webcam-based eye tracking in memory detection, I replicated three robust eye tracking studies (the cascade effect, the novelty preference, and the visual world paradigm) online using the participant's webcam as an eye tracker. Furthermore, to be able to compare lab to web, I conducted the visual world paradigm not only online using the participant’s webcam but also in the lab using a standard eye tracker.

Lastly, in the fifth chapter, I propose an alternative way to detect crime knowledge. I examined whether suspects' familiarity with a crime scene could be detected by bringing them back to it in virtual reality while changing several salient elements of it. I tested whether gaze behavior toward those modulated parts could reveal its recognition. This new method has various advantages as compared to classic memory detection, such as the fact that it could be more generally applicable as no control items are needed. The test could be presented remotely which could protect it against countermeasures. Lastly, the risk of information leakage could be lower because leakage of an entire crime scene including the modified elements is highly unlikely.

References

Ben-Shakhar, G. (2002). A critical review of the Control Questions Test (CQT). *Handbook of Polygraph Testing, 103-126.*

Ben-Shakhar, G. (2011). Countermeasures. *Memory detection: Theory and application of the Concealed Information Test*, 200-214. doi:10.1017/cbo9780511975196.012

Bradley, M. T., Barefoot, C. A., & Arsenault, A. M. (2011). Leakage of information to innocent suspects. *Memory detection: Theory and application of the Concealed Information Test*, 187-199. doi:10.1017/cbo9780511975196.011

Elaad, E. (2011). New and old covert measures in the Concealed Information Test. *Memory detection: Theory and application of the Concealed Information Test*, 114-127. doi:10.1017/cbo9780511975196.007

Fabiani, M., Karis, D., & Donchin, E. (1986). P300 and recall in an incidental memory paradigm. *Psychophysiology, 23*(3), 298-308. doi:10.1111/j.1469-8986.1986.tb00636.x

Hannula, D. E., Althoff, R. R., Warren, D. E., Riggs, L., Cohen, N. J., & Ryan, J. D. (2010). Worth a glance: using eye movements to investigate the cognitive neuroscience of memory. *Frontiers in Human Neuroscience, 4*, 166. doi:10.3389/fnhum.2010.00166

IMDb (2022, December). *Best of 2022: Top 100 TV series of 2022.* IMDb. https://www.imdb.com/best-of/top-100-tv-series-of-2022/ls566051808/

Innocence Project (2019, July 9). *Today Marks Twelve Years of Freedom for Byron Halsey.* Innocence Project. https://innocenceproject.org/cases/byron-halsey/

Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An analysis of data quality: Professional panels, student subject pools, and Amazon's Mechanical Turk. *Journal of Advertising, 46*(1), 141-155. doi:10.1080/00913367.2016.1269304

Kirkpatrick, E. A. (1894). An experimental study of memory. *Psychological Review, 1*(6),

602. doi:10.1037/h0068244

Kleinberg, B., Arntz, A., & Verschuere, B. (2019). Detecting Deceptive Intentions: Possibilities for Large-Scale Applications. *The Palgrave Handbook of Deceptive Communication,* 403-427. doi:10.1007/978-3-319-96334-1_21

Krapohl, D. J. (2011). Limitations of the Concealed Information Test in criminal cases. *Memory detection: Theory and application of the Concealed Information Test,* 151-170. doi:10.1017/cbo9780511975196.009

Lancry-Dayan, O. C., Ben-Shakhar, G., & Pertzov, Y. (2022). The promise of eye-tracking in the detection of concealed memories. *Trends in Cognitive Sciences.* doi: 10.1016/j.tics.2022.08.019

Lancry-Dayan, O. C., Nahari, T., Ben-Shakhar, G., & Pertzov, Y. (2018). Do you know him? Gaze dynamics toward familiar faces on a concealed information test. *Journal of Applied Research in Memory and Cognition, 7*(2), 291-302. doi:10.1016/j.jarmac.2018.01.011

Langleben, D. D., Schroeder, L., Maldjian, J. A., Gur, R. C., McDonald, S., Ragland, J. D., O'Brien, C. P., & Childress, A. R. (2002). Brain Activity during Simulated Deception: An Event-Related Functional Magnetic Resonance Study. *NeuroImage, 15*(3), 727–732. doi:10.1006/nimg.2001.1003

Lykken, D. T. (1959). The GSR in the detection of guilt. *Journal of Applied Psychology, 43*(6), 385. doi:10.1037/h0046060

Lykken, D. T. (1960). The validity of the guilty knowledge technique: The effects of faking. *Journal of Applied Psychology, 44,* 258-262. doi:10.1037/h0044413

Lykken, D. T. (1988). Detection of guilty knowledge: A comment on Forman and McCauley. *Journal of Applied Psychology, 73*(2), 303-304. doi:10.1037/0021-9010.73.2.303

Mandrekar, J. N. (2010). Receiver operating characteristic curve in diagnostic test assessment.

Journal of Thoracic Oncology, 5(9), 1315-1316. doi:10.1097/jto.0b013e3181ec173d

Meijer, E. H., klein Selle, N., Elber, L., & Ben-Shakhar, G. (2014). Memory detection with the Concealed Information Test: A meta-analysis of skin conductance, respiration, heart rate, and P300 data. *Psychophysiology, 51*(9), 879-904. doi:10.1111/psyp.12239

Meijer, E. H., Verschuere, B., Gamer, M., Merckelbach, H., & Ben-Shakhar, G. (2016). Deception detection with behavioral, autonomic, and neural measures: Conceptual and methodological considerations that warrant modesty. *Psychophysiology, 53*(5), 593-604. doi:10.1111/psyp.12609

Monti, M. M., Vanhaudenhuyse, A., Coleman, M. R., Boly, M., Pickard, J. D., Tshibanda, L., Owen, A. M., & Laureys, S. (2010). Willful Modulation of Brain Activity in Disorders of Consciousness. *New England Journal of Medicine, 362*(7), 579–589. doi:10.1056/nejmoa0905370

Nishimoto, S., Vu, A. T., Naselaris, T., Benjamini, Y., Yu, B., & Gallant, J. L. (2011). Reconstructing Visual Experiences from Brain Activity Evoked by Natural Movies. *Current Biology, 21*(19), 1641–1646. doi:10.1016/j.cub.2011.08.031

Oldis, D. (2017). Animating Dreams and Future Dream Recording. In *IASD Conference Abstracts.*

Osugi, A. (2011). Daily application of the Concealed Information Test: Japan. *Memory Detection: Theory and application of the Concealed Information Test*, 253-275. doi:10.1017/cbo9780511975196.015

Peth, J., Suchotzki, K., & Gamer, M. (2016). Influence of countermeasures on the validity of the Concealed Information Test. *Psychophysiology, 53*(9), 1429-1440. doi:10.1111/psyp.12690

Rosenfeld, J. P., Angell, A., Johnson, M., & Qian, J. (1991). An ERP-based, control-question lie detector analog: Algorithms for discriminating effects within individuals' average waveforms. *Psychophysiology, 38,* 319-335. doi:10.1111/j.1469-8986.1991.tb02202.x

Somers, J. (2021, November 29). *The Science of Mind Reading.* The New Yorker. https://www.newyorker.com/magazine/2021/12/06/the-science-of-mind-reading

Suchotzki, K., Verschuere, B., Van Bockstaele, B., Ben-Shakhar, G., & Crombez, G. (2017). Lying takes time: A meta-analysis on reaction time measures of deception. *Psychological Bulletin, 143*(4), 428e453. doi:10.1037/bul0000087.

Verschuere, B., Ben-Shakhar, G., & Meijer, E. (Eds.). (2011). *Memory detection: Theory and application of the Concealed Information Test.* Cambridge University Press. doi:10.1017/cbo9780511975196

Verschuere, B., Suchotzki, K., & Debey, E. (2014). Detecting deception through reaction times. *Detecting deception: Current challenges and cognitive approaches*, 269-291. doi:10.1002/9781118510001.ch12