Using the verifiability of details as a test of deception: A conceptual framework for the automation of the verifiability approach

Kleinberg, B.; Nahari, G.; Verschuere, B.

DOI
10.18653/v1/W16-0803

Publication date
2016

Document Version
Final published version

Published in
NAACL HLT 2016 : The 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies

License
CC BY

Citation for published version (APA):
Using the verifiability of details as a test of deception: A conceptual framework for the automation of the verifiability approach

Bennett Kleinberg\textsuperscript{1}, Galit Nahari\textsuperscript{2} and Bruno Verschuere\textsuperscript{1}
\textsuperscript{1} Department of Psychology, University of Amsterdam, The Netherlands.
\textsuperscript{2} Department of Criminology, Bar-Ilan University, Ramat Gan, Israel.
{b.a.r.kleinberg,b.j.verschuere}@uva.nl galit.nahari@biu.ac.il

Abstract

The Verifiability Approach (VA) is a promising new approach for deception detection. It extends existing verbal credibility assessment tools by asking interviewees to provide statements rich in verifiable detail. Details that \textit{i}) have been experienced with an identifiable person, \textit{ii}) have been witnessed by an identifiable person, or \textit{iii}) have been recorded through technology, are labelled as verifiable. With only minimal modifications of information-gathering interviews this approach has yielded remarkable classification accuracies. Currently, the VA relies on extensive manual annotation by human coders. Aiming to extend the VA’s applicability, we present a work in progress on automated VA scoring. We provide a conceptual outline of two automation approaches: one being based on the \textit{Linguistic Inquiry and Word Count} software and the other on rule-based shallow parsing and named entity recognition. Differences between both approaches and possible future steps for an automated VA are discussed.

1 Cognitive deception detection

Based on the rationale that the default setting in human communication is honesty (Levine, 2014; Verschuere & Shalvi, 2014), the cognitive approach to deception (e.g. Zuckerman et al., 1981) postulates that the act of lying requires extra mental effort compared to telling the truth (e.g. trying to fabricate a convincing lie; Vrij, 2014). The general idea of lying being correlated to increased mental effort has been corroborated by a great body of research, using self-reports, behavioral, autonomic, electrophysiological, and neural measures (Ganis et al., 2003; Verschuere et al., 2011). To further increase cognitive differences between lying and truth telling, the cognitive approach advocates applying minimal interventions in information-gathering interviewing situations that enlarge the differences between the truth tellers and liars (e.g. asking unexpected questions, asking to recall a story in reverse order; Vrij et al., 2015, Meissner et al., 2012). A recent meta-analysis indicates that cognitive techniques outperform standard interviews (Vrij et al., 2015). This body of work has also found the most reliable differences between truths and lies to be manifested in verbal rather than nonverbal behavior. Ormerod and Dando (2014), for instance, applied cognitive interviewing techniques on mock-passengers and found verbal detection methods to by far outperform its behavioral counterparts (e.g. spotting suspicious behavior). Also, objective judgments (i.e., algorithmic scoring such as discriminant analysis) outperformed human judgments (truths: 60\% vs. 80\%; lies: 64\% vs. 73\%, for human vs. objective judgments, respectively, Vrij et al., 2015). The superiority of objective criteria might be explained by the sheer amount of information for humans to take into account to derive a binary truth versus lie judgment (e.g. Rubin & Conroy, 2012).
The verbal content of statements seems to offer potential for cognition-based deception detection. Verbal deception detection offers multiple levels of analysis (e.g. overall content of statements, lexical analysis, syntactic analysis, see Fitzpatrick et al., 2015) and the most promising results of deception research fall under the umbrella term of verbal deception detection (e.g. Ott et al., 2011, 2013; Mihalcea et al., 2013; Harvey et al., 2016). Unlike other approaches, verbal deception detection is suitable for large-scale applications due to its potential for computer-automation. The cognitive approach to increasing the differences between liars and truth tellers provides a theoretical framework for a synthesis of computer-automated approaches and validated information-gathering interviewing techniques.

2 The Verifiability Approach

2.1 Rationale

Information gathering interviews typically ask the interviewee for a detailed account of the events (e.g. “Describe in as much detail as possible what happened”). Derived bottom-up from the liars’ verbal strategies (Nahari et al., 2014a), the Verifiability Approach (VA) aims to further increase the differences between liars and truth tellers. The VA is based on three assumptions about the liars’ dilemma in an interview:

1. Liars are inclined to mention sufficient details to provide a convincing false account.
2. Liars try to avoid mentioning those details that can potentially be verified by the interviewer.
3. As solution to (1) and (2), the liars provide many non-verifiable details.

Working from this dilemma, Nahari et al. (2014a) developed a set of criteria deemed appropriate as an indication of the verifiability of a detail given in a statement. Specifically, a detail is categorized as verifiable if at least one of the three criteria below applies:

- The detail describes an activity with an identifiable person.

<table>
<thead>
<tr>
<th>Type of detail</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifiable detail</td>
<td>“My husband and I parked the car outside our house and noticed our neighbour’s daughter kissing her boyfriend good-bye on their doorstep.” [with an identifiable person]</td>
</tr>
<tr>
<td></td>
<td>“There were 3 people present who witnessed me use my phone before placing it in my bag at 22:00: Ben Kleinberg, Galit Nahari, and Bruno Verschuere.” (names changed) [witnessed by an identifiable person]</td>
</tr>
<tr>
<td></td>
<td>“My phone was last used at 12.30 am in which I sent a text message to my friend who was with me that evening.” [recorded through technology]</td>
</tr>
<tr>
<td>Non-verifiable detail</td>
<td>“When I got back to my house I realised that my phone was no longer in my pocket, but had gone.”</td>
</tr>
<tr>
<td></td>
<td>“I spoke to a lady in the shop about the general chit chat of an airport, where she was going to and when her flight was.”</td>
</tr>
<tr>
<td></td>
<td>“A guy offered to buy me a drink after noticing it was my birthday.”</td>
</tr>
</tbody>
</table>

Table 1: Illustration of verifiable (criterion in square brackets) and non-verifiable details (verbatim from Vrij et al., 2016).

- The detail describes an activity that has been witnessed by an identifiable person.
- The detail describes an activity that may have been documented or recorded through technology.

Table 1 shows verbatim examples for each category from the most recent VA study (Vrij et al., 2016).

2.2 Verifiable details and verifiable facts

Hancock et al. (2005) outline that liars use more details when the nature of the deception permits it (i.e., when the narrative per se is non-verifiable). For example, opinions are inherently non-verifiable fact
scenarios. In contrast, event-based deception settings like mock-crimes are verifiable fact scenarios. In this sense, verifiable facts are interwoven with the ground truth of a deception. In its current state, the VA is appropriate only when the scenario is based on theoretically verifiable facts (e.g., a crime). In its current state, the VA is less relevant for non-verifiable fact scenarios (e.g., opinions), as one cannot verify details that are not event-based. Second, Hancock et al. (2005) discuss how liars’ verbosity could depend on the verifiability of the overall scenario. In situations where the verifiability or ground truth is difficult to establish (e.g. opinions), the liars may choose to include many details in their statement, whereas this strategy is expected to be counterproductive when the ground truth can be established. The VA extends this idea by actively challenging interviewees in different ways: liars and truth tellers are explicitly asked to provide verifiable details. This technique results in a disproportionally difficult task for the liars, whereas the truth teller can easily recall verifiable details from memory.

3 Experimental findings using the VA

In the initial experiment on the VA, Nahari et al. (2014a) modified a mock-crime procedure by instructing participants to do their normal daily business (e.g. drinking coffee, visiting a book shop) and return to the lab after 30 minutes. Upon returning to the lab, the participants were allocated to the truth-condition or the lie-condition. Those in the truth-condition were instructed to provide a truthful account of their activities in the previous 30 minutes, whereas those in the lie-condition were required to give an entirely false statement. The findings (Figure 1) show that truthful statements contained more overall details ($p < .05$) as a function of the number of verifiable details ($p < .001$). Moreover, the number of details translated to promising classification rates (Table 2). These general findings have been corroborated in several studies (e.g. Nahari & Vrij, 2014; Nahari & Vrij, 2015).

<table>
<thead>
<tr>
<th>No. of verifiable details</th>
<th>F-measure true statements</th>
<th>F-measure false statements</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.95</td>
<td>76.47</td>
<td>78.94</td>
<td></td>
</tr>
<tr>
<td>69.57</td>
<td>53.33</td>
<td>63.16</td>
<td></td>
</tr>
<tr>
<td>73.17</td>
<td>68.57</td>
<td>71.05</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: F-measures and accuracies of the VA for three decision criteria (from Nahari et al., 2014a)

From a methodological point of view, two essential elements in this study are the annotation of details in statements and subsequently the annotation of these details as either verifiable or non-verifiable.

3.1 Annotation of details

In order to extract details from the statements written by the participants, the researchers adopted the Reality Monitoring approach (RM; Sporer, 2004). RM has gained popularity in deception research because it offers a theoretical framework about content differences of true and false statements (Johnson & Raye, 1981; Vrij, 2015). The underlying assumption of RM is that true experiences are obtained through perceptual processes whereas imagined (or false) experiences are obtained through cognitive operations. This in turn is thought to be reflected in, for example, the amount and type of detail when recalling an experience. Specifically, three
of the eight RM criteria are suitable for a verifiability approach (see Nahari et al., 2014a): spatial (e.g. locations or spatial arrangements), temporal (e.g. points in time or sequence of events), and perceptual details (e.g. all sensorial information like visual information and sounds), all which truth tellers are expected to produce more of.

In Nahari et al. (2014a) two independent coders were trained in coding example statements on the three detail criteria for 2.5 hours. Within each statement, the two coders manually annotated all details that were spatial, temporal or perceptual, with an inter-rater reliability of 78%, 77%, and 78%, for perceptual, spatial and temporal details respectively. If the two coders disagreed, a third trained coder made the final decision about the presence of a detail. Consider two examples from Table 1 as illustration:

a) “My husband and I parked the car outside our house and noticed our neighbour’s daughter kissing her boyfriend good bye on their doorstep.”

b) “When I got back to my house I realised that my phone was no longer in my pocket, but had gone”

These statements are annotated as:

a) “My husband [PERCEPTUAL] and I parked [PERCEPTUAL] the car outside our house [SPATIAL] and noticed our neighbour’s daughter [PERCEPTUAL] kissing her boyfriend [PERCEPTUAL] good-bye on their doorstep [SPATIAL].”

b) “When [TEMPORAL] I got back to my house [SPATIAL] I realised that my phone was no longer in my pocket, but had gone”

Within this statement, all details that fit one of the three RM criteria are annotated. The next step in the annotation is to decide for each detail whether or not it can be deemed potentially verifiable.

### 3.2 Annotation of the verifiability of details

The annotated details were further classified as verifiable or non-verifiable (Table 1). Similar to the detail annotation, the same two independent coders made a judgment for each detail whether it fit at least one of the three verifiability criteria (see 2.1). The coders agreed on 87.95% of the detail verifiability (Nahari et al., 2014a). Each disagreement was referred to a third coder who made the final decision. After this final annotation, the overall number of details and of verifiable details was subjected to a discriminant analysis. Applied to the two examples, this phase would result in the following annotation:

a) “My husband [PERC.-VERIFIABLE] and I parked [PERC.-VERIFIABLE] the car outside our house [SPATIAL-VERIFIABLE] and noticed our neighbour’s daughter [PERC.-VERIFIABLE] kissing her boyfriend [PERC.-VERIFIABLE] good-bye on their doorstep [SPATIAL-VERIFIABLE].”

b) “When [TEMP.-NONVERIFIABLE] I got back to my house [SPATIAL-NONVERIFIABLE] I realised that my phone was no longer in my pocket, but had gone”

### 3.3 The VA information protocol

Despite the promising initial results, a key challenge to the VA is that liars can embed their lies into mainly true events, e.g., their normal daily routine (Nahari et al., 2014b), or altogether within non-verifiable scenarios (Hancock et al., 2005). For example, when using the VA on participants’ statements about false and true insurance claims, initial findings indicated that the VA does not benefit when the lies are embedded in mainly non-verifiable contexts. However, contrary to other content analysis tools (Nahari & Pazuako, 2015) the VA has been shown to allow for higher classification accuracy when the participants were aware of the working mechanisms of the tool. Harvey et al. (2016) manipulated the information liars and truth tellers received about the VA in the insurance claim setting: one group in each condition (truth vs. lie) was told to provide as much detail as possible whereas another group was informed that verifiable details are used as an indicator for truthfulness. The accuracy in the informed group (77.5%) was higher than that in the uninformed group (57.5%). This information protocol manipulation affected liars and truth tellers in
unequal ways (see 2.2) and it has now become standard procedure in VA research.

3.4 Towards large scale application of VA

Although the VA has yielded promising results in laboratory studies it is limited with regard to its large-scale applicability. Most importantly, the annotation of details and verifiability relies on manual coding making this procedure resource-intensive (e.g. Harvey et al., 2016). In other words, the manual coding of verbal criteria can be seen as a key impediment to large-scale investigations with the VA and potential applications. In the remainder of this paper, we report on a work in progress about the automation of the VA.

4 Related work on automated verbal deception detection

To put our work into perspective we briefly discuss three key studies on automated approaches to verbal deception detection. Zhou et al. (2004) conducted one of the early experimental attempts to automate the detection of deception in a computer-mediated communication eliciting lies in a group decision problem. Crucially, they found that computerized analysis added significantly to the identification of linguistic cues for the detection of deception in asynchronous settings. Mihalcea et al. (2013) answer another relevant question for the broader aim of this investigation. They showed that a data-driven machine learning approach achieved classification accuracies of up to 74% for low-stakes lies (see also Mihalcea & Strappavara, 2009). A study by Bachenko et al. (2008) complements this finding by addressing the critical issue of low-stakes with a linguistic analysis of genuine crime documents. On the one hand, they showed that a theory-based selection of cues can successfully be automated for linguistic annotation of texts, and on the other hand, they were able to develop a tagging system that discriminated true from false declaration within statements. The latter is of particular relevance for the problem of embedded lies.

5 Automating the VA

The main research question guiding this conceptual paper is whether we can automate the VA. As this is the first automated annotation approach of the VA, we will use the data of existing VA studies (e.g. Nahari et al., 2014a; Vrij et al., 2016) which will both be readily available and provide human scoring as baseline. We discuss two automation approaches that could both address the annotation of details but differ in their potential of annotating the verifiability. The first system is based on the Linguistic Inquiry and Word Count system (LIWC, Pennebaker et al., 2015) and the second system is a two-phasic annotation approach relying on named entity recognition.

5.1 LIWC-based automation

The LIWC system (Pennebaker et al., 2015) has been applied widely in psycholinguistic research (e.g. Bond & Lee, 2005; Hancock et al., 2007; Ramirez-Esparza et al., 2008). The software analyzes text statements and produces frequency tables of word categories that fit psychological processes (e.g. cognitive mechanism, affect). Bond and Lee (2005) applied LIWC to automate RM criteria in a sample of prisoners. We aim to adopt their approach to modelling the VA detail categories (perceptual, spatial, temporal) with the LIWC word categories ‘perceptual processes’ (e.g., “saw”, “heard”), ‘space’ (e.g., “down”, “under”), and ‘time’ (e.g., “before”, “until”). We will use the frequency of these word categories as proxy for overall detail in existing statements from VA studies (Table 3). Whereas we expect the annotation of details to be feasible in this system (see Bond & Lee, 2015), we

<table>
<thead>
<tr>
<th>Human coding</th>
<th>Detail annotation</th>
<th>Verifiability annotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIWC-based system</td>
<td>Word frequencies</td>
<td>Unlikely to be captured</td>
</tr>
<tr>
<td></td>
<td>of ‘perceptual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>processes’, ‘space’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and ‘time’</td>
<td></td>
</tr>
<tr>
<td>NER-based system</td>
<td>Shallow parsing of verb phrases</td>
<td>Presence of named entities as proxy for verifiability</td>
</tr>
</tbody>
</table>

Table 3: Conceptual comparison of VA automation approaches.
argue that the verifiability is less likely to be captured. The current LIWC system does not provide a word category or output that we think is able to function as proxy for detail verifiability.

5.2 Shallow parsing and NER system

In the second automation approach, we aim to develop a system adopting essentially rule-based shallow parsing (Pradhan et al., 2004) of statement activities and details that will then be coupled with named entity recognition (NER; e.g. persons, locations, organizations; Weischedel et al., 2013; Honnibal, 2016; see Appendix A). Specifically, in this first automation attempt, we aim to use the existing VA data and perform part-of-speech tag rule-based shallow parsing to annotate verb phrases as proxy for activities.

As a second step, we add the verifiability annotation using NER. By extracting named entities, we hypothesize to be able to fulfill the actual verifiability criteria (i.e., presence of or witnessing by an identifiable person and reference to technology). For example, the statements “I saw a guy in a café” contains no named entity, whereas “I saw Dan in the Starbucks” contains two named entities (Dan = PERSON, Starbucks = ORGANIZATION). Note how in both cases, LIWC and the shallow parser would identify the same detail (“saw”), but only the NER-based system would also annotate the two additional named entities. We will investigate whether the NER-added information functions as a proxy for verifiability. We aim to use Cython-based spaCy (Honnibal, 2016) software for pre-processing and annotation. The tokenizer, POS-tagger and NER algorithms are trained on the OntoNotes5 corpus (Weischedel et al., 2013).

6 Outlook and conclusion

The conceptual approach to an automation of the VA is thought to eventually enable large-scale applications. Given the novelty of the VA, the approach to its automation is still in its infancy and requires multiple phases of development. For example, it could be that the LIWC-based system and the NER-approach are not mutually exclusive but that both complement each other. A successful automation of the VA could open up new directions of verbal deception research. First, it would enable researchers to conduct VA experiments on large sample sizes and corpora sizes efficiently. Second, an automated VA could have considerable impact on applied deception research. Especially in the area of crime prevention, the practitioners’ focus is identifying the few persons out of a large population who may have false intentions. Inherent to such aims is the need for large-scale automated deception detection tools. Third, on a psycholinguistic level, the VA adds an interesting dimension to scoring mechanisms by explicitly looking at the verifiability of details. Future directions could, for example, involve modifications of the VA as a tool to identify propositions subject to ground truth checking or applying the VA to smaller units of analysis like single propositions instead of whole statements. The latter could also be a step towards detecting embedded lies.

In summary, the VA offers a promising framework for the detection of verbal deception and would benefit from automation. Two approaches were outlined, one based on the LIWC software tool and another based on named entity recognition algorithms. Successfully automated approaches of the VA could contribute to novel research paths and to further integration of cognitive deception detection and computational linguistics.

Acknowledgments

This work is supported by a grant from the Dutch Ministry of Security and Justice. We thank three critical and attentive reviewers and the editor for their invaluable input.

References


Honnibal, M. (2016). spaCy (Version 0.100.6) [Computer software]. Available from https://spacy.io/


**Appendix A**

Entities as recognized by spaCy NER algorithm (adopted from https://spacy.io/docs#annotation; most relevant categories in bold):

- **PERSON** (e.g. Bill Gates)
- **NORP** (nationalities or religious groups)
- **FACILITY** (e.g. Heathrow Airport)
- **ORG** (organization, e.g. Starbucks)
- **GPE** (countries, states, cities)
- **LOC** (locations other than GPE)
- **PRODUCT** (e.g. vehicles, food)
- **EVENT** (e.g. wars, sports events)
- **WORK_OF_ART** (title of books, songs)
- **LAW** (named documents made into laws)
- **LANGUAGE** (any named language)
- **DATE** (e.g. last week)
- **TIME** (e.g. for 2 hours)
- **PERCENT** (e.g. 85%)
- **QUANTITY** (e.g. 15kg, 42km)
- **ORDINAL** (e.g. first, second, 15th)
- **CARDINAL** (other numerals)