2012

Establishing a Foundation for Automated Human Credibility Screening

Jay F. Nunamaker Jr.
University of Arizona

Judee K. Burgoon
University of Arizona

Nathan W. Twyman
University of Arizona

Jeffrey Gainer Proudfoot
University of Arizona

Ryan M. Schuetzler
University of Nebraska at Omaha, rschuetzler@unomaha.edu

See next page for additional authors

Recommended Citation

Nunamaker, Jay F. Jr.; Burgoon, Judee K.; Twyman, Nathan W.; Proudfoot, Jeffrey Gainer; Schuetzler, Ryan M.; and Giboney, Justin Scott, "Establishing a Foundation for Automated Human Credibility Screening" (2012). *Information Systems and Quantitative Analysis Faculty Proceedings & Presentations*. 27.
https://digitalcommons.unomaha.edu/isqafacproc/27

Authors
Jay F. Nunamaker Jr., Judee K. Burgoon, Nathan W. Twyman, Jeffrey Gainer Proudfoot, Ryan M. Schuetzler, and Justin Scott Giboney

Establishing a Foundation for Automated Human Credibility Screening

Jay F. Nunamaker, Jr., Judee K. Burgoon, Nathan W. Twyman, Jeffrey Gainer Proudfoot, Ryan Schuetzler, Justin Scott Giboney
University of Arizona
Tucson, Arizona, USA
jnunamaker@cmi.arizona.edu

***Abstract*—Automated human credibility screening is an emerging research area that has potential for high impact in fields as diverse as homeland security and accounting fraud detection. Systems that conduct interviews and make credibility judgments can provide objectivity, improved accuracy, and greater reliability to credibility assessment practices, need to be built. This study establishes a foundation for developing automated systems for human credibility screening.**

Keywords-automated human credibility Screening; automated deception detection; automated detection of concealed information

I. Introduction

Systems that evaluate an individual’s truthfulness are proliferating at a faster rate than ever before. Two decades ago, the standard polygraph machine was the only mainstream “lie detector” technology. Today, lie detection systems range from handheld devices that measure vocal features to systems that involve inserting a person into a functional magnetic resonance imaging (fMRI) scanner to view activity in the brain.

Research on deception detection has likewise gained in popularity and favorability. Where deception detection research was once the purview only of cognitive psychology, we now see developed streams of deception research from fields ranging from communication, behavioral psychology, and sociology, to neuroscience, computer science, and information systems.

The drivers behind this growth are clearer now than ever before. In a world where insiders leak sensitive information, infidelity in relationships is on the rise, business scandals destroy billions in wealth, and terrorists plot to attack innocent people, systems that can effectively judge an individual’s veracity can provide value to perhaps every major aspect of our lives.

However, there are several challenges to currently used human screening techniques and technologies. The most common interviewing protocols do not enjoy scientific consensus. Additionally, technologies often require a high skill level to operate, techniques involve lengthy time requirements, and sensors can be invasive. These and similar limitations serve as barriers to more widespread application of deception detection in practice. Unfortunately, many lie detection systems ignore both established research and theoretical and protocol limitations in favor of expedience. This paper reviews literature related to automated deception detection with the goal of addressing the research question: How should key deception detection theories and protocols inform the investigation and development of automated human screening systems[1]?

The purpose of this study is to review and synthesize extant theory, protocols, and technologies that can be leveraged to advance automated human screening systems. We begin by reviewing the value of technology in human veracity screening, followed by a review of the principal theories and protocols in deception detection research. We describe the strengths and weaknesses of each in an automated screening system context. Lastly, we review technologies that have been or could be leveraged by automated human screening systems.

[1] For the context of this paper, we define *human screening system* as a unique combination of technology, actors, environment, and processes used to judge an individual’s veracity.

A. Technology in Deception Detection

Technology has been used in credibility assessment since at least 1895, when Cesare Lombroso, an Italian criminologist, used a medical device for measuring blood pressure changes during police interrogations [1]. In the 1920s and 30s, John Larson and Leonarde Keeler developed the now-widely-known polygraph machine which measures blood pressure, respiration, and skin conductance (a measure of arousal) [2].

Recently, additional technologies for human screening have been investigated including non-contact technologies for measuring heart rate and blood pressure [3], and automated vocalic [4-6], linguistic [7-9], oculometric [10-12], thermal [13, 14], and kinesic [15, 16] data capture and analysis technologies.

Technology can clearly improve deception detection accuracy. Unaided human deception detection accuracy rate hovers near chance levels [17]. However, when veracity decision makers are aided by an effective screening system, accuracy improves. There are many ways deception detection systems can improve credibility assessment accuracy. Table 1 suggests several ways in which systems can improve accuracy.

TABLE 1. HOW SYSTEMS IMPROVE DECEPTION DETECTION ACCURACY

	Tactic for Improving Veracity Judgments	Sample References
1	Detecting and measuring deception cues that humans are unable to perceive	[4, 10, 18]
2	Processing many cues simultaneously	[19]
3	Conducting complex analyses	[10, 19-21]
4	Increasing test control (e.g., using more exact timing, minimizing examiner bias)	[12, 22]
5	Persuading examiners to better use presented relevant information	[23]
6	Detecting countermeasures	[24-26]

In addition, there are other unexplored ways that technology may assist in human screening. Some of these include 1) having a virtual agent manipulate examinees in a manner that will produce stronger deception cues, 2) having a system process the most non-problematic people in a rapid screening environment automatically, freeing up time for screeners to focus on the more questionable subjects, 3) Providing examiners with insight on which topics need deeper probing, and 4) Capturing baseline data for use in future screenings.

II. DECEPTION DETECTION THEORIES APPLICABLE TO AUTOMATED SCREENING

The ability to identify deception is based on the premise that the nonverbal and verbal behaviors exhibited by truth tellers and deceivers differ. Many of these “cues to deception” can be categorized as linguistic [27, 28], vocalic [29], kinesic [30], and oculometric [31, 32] features.

Due the prevalence of deception in communication, people tend to use heuristics in an attempt to identify when deception is occurring; however, these heuristics are often inaccurate [32]. Furthermore, because of these heuristics, communicators attempt to conceal the behaviors that they perceive convey deception [32]. Research has also suggested that humans have limited cognitive capacity, suggesting that a human can only process a limited number of tasks simultaneously. When committing deception, a person may be fabricating a story while attempting to stay relaxed, making eye contact with the receiver, and conveying confidence. Our belief is that a person may be able to control some cues, and may even be highly adept at controlling those cues, however, every person has a limit to the number of cues that they can control simultaneously. Based on prior work [3, 27] we estimate that monitoring a set of 15 or more cues exceeds the threshold of cognitive ability that would be necessary to monitor and control those cues.

Several theories inform automated credibility screening, including Four-Factor Theory (FFT), Interpersonal Deception Theory (IDT), and Orienting Response (OR) theory.

Zuckerman, DePaulo, and Rosenthal [33] developed Four-Factor Theory (FFT) as an extension of the leakage hypothesis presented by Ekman and Friesen [34]. FFT more closely investigates the internal factors that can influence outward displays of deception, including: arousal, negative affect, cognitive processing, and attempted control. As deceivers attempt to control these factors, changes in behavior are likely exhibited. Cues of deception associated with these internal factors can be manifested as behaviors that are stiff, rigid, awkward, inexpressive, and lacking in spontaneity [33]. Arousal can be detected in lessened movement in the extremities [29, 30]. Negative affect can be measured by negative emotion word use [28], cognitive processing can be measured by preposition use [28], and attempted control can be measured by pupil dilation or voice pitch [32]. All of these cues can be measured using automated sensors.

Interpersonal Deception Theory (IDT) [35] further subdivides Ekman's deception cues into strategic and nonstrategic behaviors. *Strategic cues* are planned behaviors that occur because the deceiver wishes to appear truthful. An example of strategic cues would be the messages that the deceiver intends to send. Attributes of the message such as length and word choice may be used to identify deception, even though these messages are crafted consciously by the deceiver in an attempt to appear truthful. *Nonstrategic cues*, on the other hand, are unintentional behaviors occurring as a byproduct of deception. Many of the cues used in automated deception detection fall into the category of nonstrategic cues. Pupil dilation, changes in the voice, and postural shifts are all nonstrategic indicators of deception.

A large part of automated deception detection is based upon behavioral research on the orienting response [36, 37]. The orienting response is an autonomic reaction to a personally relevant stimulus [37]. This response is highly relevant with eye movement [38]. When there is a visual stimulus, the eyes naturally and almost instantly move to the stimulus without any cognitive effort. Using this theory allows an automated screener to present visual stimuli that are more salient for the target individual, resulting in measurable changes in gaze behavior that can be used to identify recognition.

Another area of investigation in deception detection research is a mechanism we term defensive responding. While the OR is thought to be a reaction to any novel or personally significant stimulus, defensive responding only occurs when that stimuli is perceived to be aversive.

III. Deception Detection Protocols for Automated Screening

The most common formalized methods for detecting deception include the Control Question Technique (CQT) [39], the Behavioral Analysis Interview (BAI) [40], and the Concealed Information Test (CIT) [41, 42]. Automated screening can mimic these interviewing protocols in full, or it can develop alternative protocols that may better serve an automated screening context.

There is a benefit to mimicking existing protocols or portions of these protocols that have theoretical and empirical support. However, there are limitations to existing interview protocols. The CQT, while it is the most widely used, requires hours to complete. The BAI can also require an hour or more. Furthermore, both techniques require a high level of interviewing skill in terms of manipulating the beliefs of the examinee and following up on contextually significant details in responses [43]. These skills are difficult to effectively mimic. Thus, in deception detection contexts, where time and cost are key factors, alternative interviewing protocols are likely more effective.

The CIT was developed as an alternative approach to conducting criminal interviews [25]. The premise of the CIT is that it tests a person's recognition of stimuli that only an individual associated with a given crime or incident would be aware of. The scientific underpinnings of the CIT are grounded in the orienting response [44], which results in physiological responses to recognized stimuli that will be larger than physiological responses to unrecognized stimuli. Individuals with no knowledge of a given incident are expected to respond to all stimuli randomly.

Furthermore, the CIT is a promising protocol for rapid or secondary screening. It requires virtually no skill on the part of the interviewer, enjoys wide scientific consensus on validity, and has a simple format that can be more easily automated. Though it is the least commonly used technique in practice, some researchers believe the CIT can and should be employed more widely [45].

IV. Non-invasive Technologies for Automated Deception Detection

Important to automated screening research is the identification and development of noninvasive means to detect deception. Below we discuss the different technologies used for gathering information about deception without the need for invasive sensors such as those used in the polygraph. These technologies include automated vocalic, kinesic, oculometric, thermal, and linguistic data capture and analysis.

A. Vocalics

The voice is a rich source of information. Some of the vocal cues important to the automated detection of deception are voice quality, pitch, and response latency. These three measures are reliable indicators of either the stress or cognitive load associated with deception. The voice has been studied extensively as it relates to the communication and understanding of emotion [46, 47].

Voice quality can be defined as the harmonics-to-noise ratio present in a given vocal recording [48]. Deception research investigating variances in voice quality associated with truth and deception suggest that liars tend to speak with a lower harmonic-to-noise ratio than those telling the truth [3]. This variance can be attributed to increased cognitive effort and the influence of stress and emotion [49].

The *pitch* of the voice, or the fundamental frequency at which someone is speaking, is controlled by contractions of the larynx in the throat. It is closely related to tension, and thus increases in stress or nervousness increase the pitch of the speaker's voice [31]. Attributes of a person's pitch that can be used in understanding emotion include the average pitch during an utterance, as well as the variability in pitch over the length of the utterance [46].

Typically measured in milliseconds, *response latency* is the length of time between when a question is asked and when the person begins to respond. Response latency is an important indicator of cognitive load [50]. Increased cognitive load is one of the theoretical bases for the detection of deception [51-53]; we use cognitive load indicated by increased response latency as a cue of deception.

B. Kinesics and Proxemics

The kinesic and proxemic indicators of deception are many and varied. A meta-analysis found some support for using lip presses, chin raises, fidgeting, illustrators, facial pleasantness, and overall tension ratings for differentiating truth from deception [31]. However, the effectiveness of these cues appear to be moderated by motivation level [31], and is likely moderated by culture, context, question type, personality, and situational factors. For instance, different cultures have different tendencies in displaying facial pleasantness, and chin raises during a response may have different meanings depending on the nature of the question asked.

Thus, when systems incorporate kinesic cues to deception, it is critical that the system include a protocol designed to control for or at least minimize the effects of moderating factors.

A more immediate challenge for incorporating kinesics into automated screening systems is the automation itself. In traditional research into non-verbal behavior, human judges review video recordings of individuals and manually notate each movement. To automate this approach, some researchers have developed methods of capturing body and facial movement by using computer vision techniques to track the location of points on the body over time. Abstract variables derived from this approach have proven somewhat effective in discriminating high from low veracity; however, a mapping of these automatically generated cues to specific motions and gestures is still needed.

An alternative but similar approach focused on the lack of movement, or rigidity [16]. Rigidity is a common correlate of deception, and some evidence suggests it may be difficult to control [52]. Individuals under conditions of low veracity exhibit less overall movement, and the movement that does occur appears forced (i.e., movements are shorter in duration and have greater velocity) [52, 54, 55]. Using computer vision techniques, Twyman measured overall movement during a CIT, where no communicative movement is present. An overall decrease in movement during target items was found among deceptive individuals [12].

C. Oculometrics

The eyes offer a rich set of cues for deception. Pupil dilation, blinking patterns, and eye movement can each be influenced by behavioral and physiological correlates of deception.

Pupil dilation has been shown to be associated with deception in many different contexts [56-58]. The dilation of the pupil varies not only with changes in light, but also with cognitive processing [59], memory load [60], orienting reflexes [56-58], and attention and effort [61].

Eye movement is likewise influenced by cognitive and affective factors. A number of studies have investigated the use of eye gaze fixation points to identify familiarity with faces. Ellis and colleagues [62] and Althoff and Cohen [63] both explored the interpretation of eye gaze fixation patterns on internal and external facial features to identify familiarity. The results of these studies were orthogonal. Stacey and colleagues [64] leveraged a similar approach to identifying familiarity, but were similarly unable to discriminate between familiar and unfamiliar face processing.

Additional work has been done to tie eye movement patterns to deception and concealed knowledge. The protocols employed in this initial work have included a memory effects testing protocol [65], the CQT [11], the CIT [12, 66, 67], and novel methods for detecting hidden knowledge [68].

D. Linguistics

There has been much interest in employing automated linguistic analysis to deception detection. A meta-analysis of linguistic cues revealed that response detail, plausibility, logical structure, discrepancies, involvement, immediacy, and repetitions, as well as spontaneous corrections, admissions of lack of memory, and related external associations may be useful indicators of deception [31]. Some of these cues are still questionable (a result of non-homogeneity in surveyed studies), and additional cues may be significant, but only during certain contexts and under particular circumstances.

In automated screening, the current state of technology is such that not all promising linguistic cues can be automatically extracted. For instance, an understanding of contextual meaning and situational norms is required to determine the plausibility of a response. While natural language processing techniques are making strides in understanding semantics, there is still much work to be done before systems will be able to make such a judgment such as plausibility with an acceptable level of reliability.

Some research on automated linguistic analysis for deception detection has found support for many of the linguistic features identified in DePaulo [31], while other research has found additional or in some cases conflicting results. For linguistic analysis, it may be important to consider whether the response is verbal or written, the context of the questioning, and the type of questions asked. It seems likely that culture and personality factors also play an important role. For this reason, results obtained from linguistic analysis should be considered in light of these factors.

There are also technology limitations to employing automated linguistic analysis to deception detection. In a screening scenario, words are usually spoken rather than written. Most, if not all, current automated transcription technologies require calibration to an individual's voice before an acceptable level of automated transcription accuracy can be obtained. Such calibration may be a reasonable addition to extended screening, but the additional time requirement would likely preclude application to rapid screening applications. An exception might be if individuals are expected to be screened often by the same system, such as when entering a secure facility regularly for work. In such cases, an initial voice calibration process would be the only requirement for capturing usable data for linguistic analysis.

E. Cardiorespiratory measures

Pulse rate, blood pressure, and respiration rate are all physiological cues that have been shown to have a reliable association with deception [69, 70]. These vary with deception because of the increased stress and cognitive load associated with the process of deceiving and monitoring the interaction. A Laser Doppler Vibrometer (LDV) is a device that directs a medically safe laser on the neck of a user and is capable of reporting the pulse, blood pressure, and respiration rate of an individual without the need to attach a sensor to the body. Pulse, blood pressure, and respiration rate are gathered through the measurement of vibrations on the surface of the skin.

Derrick et al. [71] investigated the use of the LDV in uncovering deception and found an accuracy rate of 64%, indicating that it is not suitable to be used alone. However, in combination with the other sensors and cues discussed above, the LDV may be able to provide a valuable piece of information in discovering deception. Furthermore, the addition of cardio-respiratory measures could provide further insight into the mental and emotional state of interviewees.

Current LDV technology, however, is not ready for a fully automated environment. A few key issues identified in [71] are as follows: (1) An operator is required to initially aim the laser at the interviewee, (2) A clear line of sight to the neck is required, meaning that some articles of clothing may impede the ability to use this sensor, and (3) only the pulse rate can be reported in real-time, while blood pressure and respiration are recorded only after post-processing. When these issues can be addressed, it may be advisable to reconsider the LDV for inclusion in an automated screening environment.

Other covert measures of respiration have also been investigated for their effectiveness in detecting deception [72]. The in-seat and backrest respiration sensors used in this experiment were able to measure respiratory rates much more subtly than the pneumographs used in polygraph interviews, while achieving similar levels of accuracy. These sensors, though, are limited in that they require the interviewee to be seated. However, if the context of the automated screening allows for sitting participants, such a device would be useful in obtaining respiration information unobtrusively.

F. Thermal measures

The use of thermal imaging to detect cues of deception is a relatively novel area of investigation. In this context, thermal imaging is widely used to identify increases in regional facial blood flow in the orbital areas surrounding the eyes [13, 14]. A number of studies have also used thermal imaging to monitor temperature changes in the forehead [73, 74]. One proposed mechanism triggering these changes is the fight or flight response [14]. As a part of this response, blood is distributed across the body to skeletal muscles [14]. Another proposed trigger is the orienting response [37, 75].

Contributing to the surge of interest in this area is the potential to measure cues of deception noninvasively. This is a critical differentiation from the widely-used polygraph examination. A noninvasive tool will allow thermal data to be collected both overtly and covertly [76]. Furthermore, changes in blood distribution and localized elevated temperature are controlled by the sympathetic nervous system, thus, this autonomic response is likely resistant to countermeasures [77].

Research evaluating the accuracy rate of thermal-based deception detection is promising. Pavlidis [13] and colleagues conducted a mock-crime experiment during which subjects assaulted and stole money from a dummy. Using thermal imaging data to discriminate between guilty and innocent subjects yielded a classification accuracy rate of 83%. A different study tested both startle and mock-crime experiments and reported a classification accuracy rate of 87.2% [78]. Finally, Zhu and colleagues [74] examined the accuracy rate of thermal imaging by monitoring the corrugator muscle in the forehead, and reported a classification accuracy rate of 76.3%. Despite the promising findings in each of these studies, others argue that thermal imaging is not feasible for rapid screening.

Vrij [79] points out a number of obstacles. First, the assumption is made that all deceivers will demonstrate stress cues, which may be prevalent but not ubiquitous. Second, there is a limited corpus of research investigating the types of interviewing techniques that would prove useful for rapid screening. Third, accuracy rates close to 90% in the lab are promising, but a 10% inaccuracy rate would result in an alarming number of false positives in a field setting.

Despite these criticisms, future research is needed to determine if using thermal imaging is a viable tool to identify cues of deception and recognition, especially when used in conjunction with other sensors.

V. INVASIVE MEASURES FOR DETECTING DECEPTION

Although our emphasis has been on noninvasive methods for detecting deception, advances in cognitive neuroscience have led to investigations using more invasive technologies such as fMRI and electroencephalograms (EEGs) that measure brain functioning during deceptive responding, states of high stress or cognitive overload [e.g., 18, 80-83]. The fMRI measures brain activity from changes in blood flow in regions of the brain. The EEG measures electrical activity and event-related potentials such as responses to “oddball” stimuli. These technologies, which are cumbersome, expensive, and time-consuming to implement, are not feasible for rapid screening but can be used to cross-validate other noninvasive approaches. For example, they can demonstrate whether the “executive” region of the brain in the prefrontal cortex becomes engaged during a deceptive narrative or whether novel stimuli presented during a CIT alter brain wave patterns, thus providing insights into how the brain produces and processes deception.

VI. OUR APPROACH

To address the need for automated human credibility screening without sacrificing scientific rigor, we have begun a stream of research on automated human screening using a kiosk-based approach. We have generally relied on a design science approach, which focuses on building and evaluating new IT artifacts to extend knowledge [84].

The first phase of our approach was identifying sensors that could collect cues of deception and concealed knowledge in a rapid, non-invasive screening context. A variety of experimental tasks have been used to test and calibrate the sensors, including: mock-crime experiments, simulated screening experiments, and automated screening interviews using embodied agents. More than 2000 subjects have participated in these studies.

A first-generation kiosk was created with the intention to demonstrate a proof-of-concept. It served as a framework for testing sensors and incorporating the first attempt at using an embodied agent to conduct automated interviews. Its dynamic design allowed ease in adding, removing and calibrating sensors.

A second iteration, termed the Automated Virtual Agent for Truth Assessments in Real Time (AVATAR) was designed to incorporate additional sensors and other features relevant to deployment in the field, including a biometric fingerprint scanner, an RFID passport reader, and a magnetic strip reader for processing fees [3]. To collect data to improve future designs of the AVATAR, a field test at a U.S. Customs and Border Protection (CBP) office in Nogales, Arizona was conducted, and data from that field test is currently being analyzed.

To facilitate iterative kiosk design, building, and experimentation, we also developed an Automated Screening Kiosk (ASK) that is modular and easily changeable. The ASK has already been successfully used in several experiments utilizing a CIT paradigm [12].

VII. CURRENT CHALLENGES AND FUTURE DIRECTIONS

Because this is a new area of research, there are many challenges to be addressed. These challenges range from experimental considerations to ensure validity to policy considerations to ensure compliance with law. A sampling of these challenges is listed in Table 2.

TABLE 2. AUTOMATED CREDIBILITY SCREENING SYSTEM RESEARCH CHALLENGES

Challenge		Challenge Description
1	Ensuring Realism in Experimental Research	Since credibility cues are linked to cognitive and behavioral reactions to real-world theoretical constructs, it is important to replicate those theoretical constructs realistically in the laboratory or results will not generalize.
2	Integrating System and Human Judgment	In many scenarios, a credibility system judgment will inform or otherwise be merged with a human judgment. There is some evidence of potential for loss of effectiveness as a result. How can the correct outcome be best assured in these situations?
3	Minimizing or Controlling for Environmental Factors	While many credibility assessments usually occur in a closed room with few distractions, those that occur as part of a job interview, forensic accounting interview, or rapid screening interview may take place in a noisy environment that could affect sensors, responses, and interactions.
4	Minimizing or Controlling for Cultural or Personality Factors	In few cases will a physiological or behavioral response be culture or personality agnostic. Further research needs to discover how relevant cultural norms and personality traits affect cues to deception in various contexts.
5	Detecting or Minimizing the Effectiveness of Countermeasures	Countermeasures are methods examinees employ to try and trick a credibility assessment into generating a truthful judgment. Countermeasures has long been an important area of research in deception detection, but new methods and measures introduce additional complexities.
6	Increasing Accuracy of Automated Transcription	Linguistic measures of deception show great promise, but in many credibility assessment contexts only verbal responses are recorded, or typed or written responses are not feasible. In such cases, automated transcription will be necessary to take advantage of these linguistic cues. Automatic transcription increases in difficulty when no training set is available or possible to obtain or when background noise is present.
7	Adjusting Models for Different Base Rates	Most experimental research in deception detection uses a parametric design. However, real-world applications may have much different positive rates, and models will need to be adjusted to account for these differences.
8	Designing Effective Protocols for Field Experiments	A major challenge with field experiments is establishing ground truth. That is, it is difficult to determine actual credibility a priori or ex post facto, so that system judgments can be compared to known fact. Effective field experimental protocols will need to obtain ground truth or be able to effectively estimate it.
9	Visualizing System Output for Decision Support	Automated Credibility Screening Systems have the potential to produce a large amount of input for decision makers. How to best present this information to decision makers and managers is an open question for future research.
10	Integrating so as to decrease, rather than increase decision time	A key goal of most automated credibility systems is to reduce manual labor. Especially in rapid screening contexts, systems will need to be designed such that throughput will at least not decrease, but potentially increase through fully automated processing of the least risky examinees.
11	Adapting to account for Psychological Deficiencies	How psychological deficiencies such as psychopathy may affect automated credibility assessment systems is an open research question. Related research suggests that it is an important area to address.
12	Ensuring Proper Training for Different Types of Users	Some decision makers such as rapid screening officers will be interacting with these systems on a regular basis, while others such as small business hiring committees will use them infrequently. There is a risk of improper use or disuse among users of different personality types and dispositions. How should training be adapted for each context?
13	Addressing Corporate and Municipal Policy Concerns	Privacy is an important concern. The United States Supreme Court has forbidden the use of the standard polygraph to screen applicants, except for government positions. What will be the challenges to public acceptance of this new technology, and how can these challenges be addressed while ensuring privacy and security of personal data?

While the challenges are complex and diverse, they can be used to help guide future research. First, the accuracy rates of technologies used to identify cues of deception and concealed knowledge must be tested, and ultimately improved, by conducting laboratory experiments promoting realism and generalizability. This will require additional research testing the sensors discussed in this paper, as well as identifying new sensors that are feasible and relevant for rapid, noninvasive credibility assessments. Second, the realism and dynamism of embodied agents used to conduct the automated interviews must be improved. As embodied agents become more effective, they can be used more efficiently to elicit information, foster trust and credibility, and ultimately, improve the accuracy of the system as a whole. Third, prior research suggests that users of decision support systems often disregard the recommendations provided to them. Thus, additional research is needed to investigate the way in which such systems could foster credibility with end users, and ultimately, provide value to the organization. Fourth, transitioning such a system from development to use in the field will require additional considerations regarding information privacy, securing data compiled by sensors, and overcoming obstacles imposed by government and municipal policies that may hinder implementation.

VIII. CONCLUSIONS

There are many potential applications for technologies that can conduct automated credibility assessments. In light of this, a variety of research streams continue to be investigated, including identifying and testing sensors to identify deception and concealed knowledge, improving data fusion and analysis techniques, and creating embodied agents to conduct automated interviews. Combining the findings from these diverse areas of exploration will result in robust platforms that can more accurately assess credibility.

REFERENCES

[1] P. V. Trovillo, “A history of lie detection,” *Journal of Criminal Law and Criminology,* vol. 29, pp. 848-881, 1939.

[2] K. Alder, “To Tell the Truth: The Polygraph Exam and the Marketing of American Expertise,” *Historical Reflections,* vol. 24, no. 3, pp. 487-525, 1998.

[3] J. F. Nunamaker, D. C. Derrick, A. C. Elkins *et al.*, “Embodied Conversational Agent–Based Kiosk for Automated Interviewing,” *Journal of Management Information Systems,* vol. 28, no. 1, pp. 17-48, 2011.

[4] A. C. Elkins, and J. K. Burgoon, "Validating Vocal Analysis Software to Assess Credibility in Interpersonal Interaction: A Multilevel Factor Analytic Approach."

[5] M. Gamer, H. G. Rill, G. Vossel *et al.*, “Psychophysiological and vocal measures in the detection of guilty knowledge,” *International Journal of Psychophysiology,* vol. 60, no. 1, pp. 76-87, 2006.

[6] J. D. Harnsberger, H. Hollien, C. A. Martin *et al.*, “Stress and Deception in Speech: Evaluating Layered Voice Analysis,” *Journal of Forensic Sciences,* vol. 54, no. 3, pp. 642-650, May, 2009.

[7] C. M. Fuller, D. P. Biros, and R. L. Wilson, “Decision support for determining veracity via linguistic-based cues,” *Decision Support Systems,* vol. 46, no. 3, pp. 695-703, Feb, 2009.

[8] L. M. Vizer, L. Zhou, and A. Sears, “Automated stress detection using keystroke and linguistic features: An exploratory study,” *International Journal of Human-Computer Studies,* vol. 67, no. 10, pp. 870-886, Oct, 2009.

[9] L. Zhou, and D. Zhang, “Following linguistic footprints: Automatic deception detection in online communication,” *Communications of the Acm,* vol. 51, no. 9, pp. 119-122, Sep, 2008.

[10] K. Fukuda, “Eye blinks: New indices for the detection of deception,” *International Journal of Psychophysiology,* vol. 40, no. 3, pp. 239-245, 2001.

[11] D. B. Osher, “Multimethod assessment of deception: Oculomotor movement, pupil size, and response time measures.,” Department of Educational Psychology, University of Utah, Salt Lake City, Utah, USA, 2007.

[12] N. W. Twyman, “Automated Human Screening for Detecting Concealed Information,” Department of Management Information Systems, University of Arizona, Tucson, AZ, 2012.

[13] I. Pavlidis, N. L. Eberhardt, and J. A. Levine, “Seeing through the face of deception,” *Nature,* vol. 415, no. 6867, pp. 35-35, 2002.

[14] I. Pavlidis, and J. Levine, "Thermal facial screening for deception detection." pp. 1143-1144.

[15] T. O. Meservy, M. L. Jensen, J. Kruse *et al.*, “Deception detection through automatic, unobtrusive analysis of nonverbal behavior,” *IEEE Intelligent Systems,* vol. 20, no. 5, pp. 36-43, 2005.

[16] N. W. Twyman, A. Elkins, and J. K. Burgoon, "A Rigidity Detection System for the Guilty Knowledge Test."

[17] C. F. Bond, and B. M. DePaulo, “Accuracy of deception judgments,” *Personality and Social Psychology Review,* vol. 10, no. 3, pp. 214-234, 2006.

[18] M. Gamer, T. Bauermann, P. Stoeter *et al.*, “Covariations among fMRI, skin conductance, and behavioral data during processing of concealed information,” *Human Brain Mapping,* vol. 28, no. 12, pp. 1287-1301, 2007.

[19] D. C. Derrick, A. C. Elkins, J. K. Burgoon *et al.*, “Border Security Credibility Assessments via Heterogeneous Sensor Fusion,” *IEEE Intelligent Systems,* vol. 25, no. 3, pp. 41-49, 2010.

[20] M. Gamer, B. Verschuere, G. Crombez *et al.*, “Combining physiological measures in the detection of concealed information,” *Physiology & Behavior,* vol. 95, no. 3, pp. 333-340, 2008.

[21] K. Moffitt, Elkins, A. C., Burgoon, J. K., Nunamaker, J. F., Jr., "Rapid Noncontact Credibility Assessment via Linguistic/Vocalic Analyses."

[22] B. Verschuere, G. Crombez, T. Degrootte *et al.*, “Detecting Concealed Information with Reaction Times: Validity and Comparison with the Polygraph,” *Applied Cognitive Psychology,* vol. 24, no. 7, pp. 991-1002, Oct, 2010.

[23] M. L. Jensen, P. B. Lowry, J. K. Burgoon *et al.*, “Technology dominance in complex decision making: The case of aided credibility assessment,” *Journal of Management Information Systems,* vol. 27, no. 1, pp. 181-207, 2010.

[24] E. Elaad, and G. Ben-Shakhar, “Countering Countermeasures in the Concealed Information Test Using Covert Respiration Measures,” *Applied Psychophysiology and Biofeedback,* vol. 34, no. 3, pp. 197-208, 2009.

[25] D. T. Lykken, “THE VALIDITY OF THE GUILTY KNOWLEDGE TECHNIQUE - THE EFFECTS OF FAKING,” *Journal of Applied Psychology,* vol. 44, no. 4, pp. 258-262, 1960, 1960.

[26] J. P. Rosenfeld, and E. Labkovsky, “New P300-based protocol to detect concealed information: Resistance to mental countermeasures against only half the irrelevant stimuli and a possible ERP indicator of countermeasures,” *Psychophysiology,* vol. 47, no. 6, pp. 1002-1010, Nov, 2010.

[27] L. Zhou, J. K. Burgoon, D. P. Twitchell *et al.*, “A comparison of classification methods for predicting deception in computer-mediated communication,” *Journal of Management Information Systems,* vol. 20, no. 4, pp. 139-165, 2004.

[28] J. Masip, M. Bethencourt, G. Lucas *et al.*, “Deception detection from written accounts,” *Scandinavian Journal of Psychology,* vol. 53, no. 2, pp. 103-111, 2012.

[29] S. L. Sporer, and B. Schwandt, “Moderators of nonverbal indicators of deception,” *Psychology, Public Policy, and Law,* vol. 13, no. 1, pp. 1-34, 2007.

[30] M.-A. Reinhard, and S. L. Sporer, “Listening, not watching: Situational familiarity and the ability to detect deception,” *Journal of Personality and Social Psychology,* vol. 101, no. 3, pp. 467-484, 2011.

[31] B. M. DePaulo, J. J. Lindsay, B. E. Malone *et al.*, “Cues to deception,” *Psychological Bulletin,* vol. 129, no. 1, pp. 74-118, Jan, 2003.

[32] M. Hartwig, and C. F. Bond, “Why do lie-catchers fail? A lens model meta-analysis of human lie judgments,” *Psychological Bulletin,* vol. 137, no. 4, pp. 643-659, 2011.

[33] M. Zuckerman, B. M. DePaulo, and R. Rosenthal, “Verbal and nonverbal communication of deception,” *Advances in Experimental Social Psychology,* vol. 14, no. 1, pp. 1-59, 1981.

[34] P. Ekman, and W. V. Friesen, “Nonverbal Leakage and Clues to Deception,” *Psychiatry,* vol. 32, no. 1, pp. 88-&, 1969.

[35] D. B. Buller, and J. K. Burgoon, “Interpersonal deception theory,” *Communication Theory,* vol. 6, no. 3, pp. 203-242, 1996.

[36] I. P. Pavlov, *Condition Reflex*, Oxford, England: Clarendon Press, 1927.

[37] E. N. Sokolov, “Higher Nervous Functions - Orienting Reflex,” *Annual Review of Physiology,* vol. 25, no. 1, pp. 545-580, 1963.

[38] J. G. Proudfoot, N. W. Twyman, and J. K. Burgoon, "Familiarity recognition in automated screening environments: Utilizing eye-tracking technology as an intelligence-gathering tool."

[39] D. C. Raskin, and C. R. Honts, "The Comparison Question Test," *Handbook of Polygraph Testing*, M. Kleiner, ed., Academic Press, 2002, pp. 1-47.

[40] F. Horvath, J. P. Blair, and J. P. Buckley, “The Behavioral Analysis Interview: Clarifying the Practice, Theory, and Understanding of its use and effectiveness,” *International Journal of Police Science & Management,* vol. 10, no. 1, pp. 101-118, 2008.

[41] Author ed.^eds., “Practical Use of the Concealed Information Test for Criminal Investigation in Japan,” *Handbook of Polygraph Testing*, San Diego, CA, USA: Academic Press, 2002, p.^pp. Pages.

[42] D. T. Lykken, “The GSR in the Detection of Guilt,” *Journal of Applied Psychology,* vol. 43, no. 6, pp. 385-388, 1959.

[43] A. Vrij, *Detecting Lies and Deceit: Pitfalls and Opportunities*, Second ed., West Sussex, England: John Wiley & Sons, Ltd, 2008.

[44] B. Verschuere, G. Crombez, A. D. Clercq *et al.*, “Autonomic and behavioral responding to concealed information: Differentiating orienting and defensive responses,” *Psychophysiology,* vol. 41, no. 3, pp. 461-466, 2004.

[45] W. G. Iacono, "Encouraging the use of the Guilty Knowledge Test (GKT): what the GKT has to offer law enforcement," *Memory Detection: Theory and Application of the Concealed Information Test*, B. Verschuere, G. Ben-Shakhar and E. Meijer, eds., New York, NY, USA: Cambridge University Press, 2011.

[46] K. R. Scherer, “Vocal affect expression: A review and a model for future research,” *Psychological Bulletin,* vol. 99, no. 2, pp. 143-165, 1986.

[47] R. Banse, and K. R. Scherer, “Acoustic profiles in vocal emotion expression,” *Journal of Personality and Social Psychology,* vol. 70, no. 3, pp. 614-636, 1996.

[48] P. Boersma, "Accurate short-term analysis of the fundamental frequency and the harmonics-to-noise ratio of a sampled sound." pp. 97-110.

[49] A. C. Elkins, D. C. Derrick, and M. Gariup, "The Voice and Eye Gaze Behavior of an Imposter: Automated Interviewing and Detection for Rapid Screening at the Border."

[50] W. E. Hockley, “Analysis of response time distributions in the study of cognitive processes,” *Journal of Experimental Psychology: Learning, Memory, and Cognition,* vol. 10, no. 4, pp. 598-615, 1984.

[51] A. Vrij, S. A. Mann, R. P. Fisher *et al.*, “Increasing cognitive load to facilitate lie detection: The benefit of recalling an event in reverse order,” *Law and Human Behavior,* vol. 32, no. 3, pp. 253-265, Jun, 2008.

[52] A. Vrij, G. R. Semin, and R. Bull, “Insight into behavior displayed during deception,” *Human Communication Research,* vol. 22, no. 4, pp. 544-562, Jun, 1996.

[53] D. P. Dionisio, E. Granholm, W. A. Hillix *et al.*, “Differentiation of deception using pupillary responses as an index of cognitive processing,” *Psychophysiology,* vol. 38, no. 2, pp. 205-211, 2001.

[54] D. B. Buller, and R. K. Aune, “Nonverbal cues to deception among intimates, friends, and strangers,” *Journal of Nonverbal Behavior,* vol. 11, no. 4, pp. 269-290, 1987.

[55] A. Vrij, “Behavioral Correlates of Deception in a Simulated Police Interview,” *Journal of Psychology,* vol. 129, no. 1, pp. 15-28, Jan, 1995.

[56] J. C. Nunnally, P. D. Knott, A. Duchnowski *et al.*, “Pupillary response as a general measure of activation,” *Attention, Perception, & Psychophysics,* vol. 2, no. 4, pp. 149-155, 1967.

[57] S. Nieuwenhuis, E. J. De Geus, and G. Aston-Jones, “The anatomical and functional relationship between the P3 and autonomic components of the orienting response,” *Psychophysiology,* vol. 48, no. 2, pp. 162-175, 2011.

[58] B. C. Goldwater, “Psychological significance of pupillary movements,” *Psychological Bulletin,* vol. 77, no. 5, pp. 340-355, 1972.

[59] J. Beatty, and B. L. Wagoner, “Pupillometric signs of brain activation vary with level of cognitive processing,” *Science,* vol. 199, no. 4334, pp. 1216-1218, 1978.

[60] D. Kahneman, and J. Beatty, “Pupil diameter and load on memory,” *Science,* vol. 154, no. 3756, pp. 1583-1585, 1966.

[61] D. Kahneman, *Attention and Effort*, Englewood Cliffs, NJ: Prentice-Hall Inc., 1973.

[62] H. D. Ellis, J. W. Shepherd, and G. M. Davies, “Identification of familiar and unfamiliar faces from internal and external features,” *Perception,* vol. 8, no. 4, pp. 431-439, 1979.

[63] R. R. Althoff, and N. J. Cohen, “Eye-movement-based memory effect: A reprocessing effect in face perception,” *Journal of Experimental Psychology: Learning, Memory, and Cognition,* vol. 25, no. 4, pp. 997-1010, 1999.

[64] P. C. Stacey, S. Walker, and J. D. M. Underwood, “Face processing and familiarity: Evidence from eye-movement data,” *British Journal of Psychology,* vol. 96, no. 4, pp. 407-422, 2005.

[65] N. W. Twyman, K. Moffitt, J. K. Burgoon *et al.*, "Using Eye Tracking Technology as a Concealed Information Test ".

[66] C. Schwedes, and D. Wentura, “The revealing glance: Eye gaze behavior to concealed information,” *Memory & Cognition*, pp. 1-10, 2011.

[67] J. D. Ryan, D. E. Hannula, and N. J. Cohen, “The obligatory effects of memory on eye movements,” *Memory,* vol. 15, no. 5, pp. 508-525, 2007.

[68] D. C. Derrick, K. Moffitt, and J. F. Nunamaker, "Eye Gaze Behavior as a Guilty Knowledge Test: Initial Exploration for Use in Automated, Kiosk-based Screening."

[69] G. H. Barland, and D. C. Raskin, “An evaluation of field techniques in detection of deception,” *Psychophysiology,* vol. 12, pp. 321-330, 1975.

[70] R. J. Cutrow, “The objective use of multiple psychological indices in the detection of deception,” *Psychophysiology,* vol. 9, pp. 578-588, 1972.

[71] D. C. Derrick, A. C. Elkins, and J. K. Burgoon, "Cardiovascular responses during mock crime interviews: Assessment using Laser Doppler Vibrometry."

[72] E. Elaad, and G. Ben-Shakar, “Covert respiration measures for the detection of concealed information,” *Biological Psychology,* vol. 77, no. 3, pp. 284-291, 2008.

[73] C. Puri, L. Olson, I. Pavlidis *et al.*, "StressCam: non-contact measurement of users' emotional states through thermal imaging." pp. 1725-1728.

[74] Z. Zhen, P. Tsiamyrtzis, and I. Pavlidis, "Forehead thermal signature extraction in lie detection." pp. 243-246.

[75] J. M. C. Vendemia, “Detection of Deception,” *Polygraph,* vol. 32, no. 2, pp. 97-106, 2003.

[76] A. Vrij, and P. A. Granhag, "Interviewing to Detect Deception," *Offenders' Memories of Violent Crimes*, pp. 279-304: John Wiley & Sons, 2008.

[77] P. H. Tu, G. Doretto, N. O. Krahnstoever *et al.*, “An intelligent video framework for homeland protection,” *The International Society for Optical Engineering,* vol. 6562, 2007.

[78] P. Tsiamyrtzis, J. Dowdall, D. Shastri *et al.*, “Imaging facial physiology for the detection of deceit,” *International Journal of Computer Vision,* vol. 71, no. 2, pp. 197-214, 2007.

[79] A. Vrij, "Detecting Deception," *Practical Psychology for Forensic Investigations and Prosecutions*, pp. 89-102: John Wiley & Sons, 2008.

[80] G. Ganis, J. P. Rosenfeld, J. Meixner *et al.*, “Lying in the scanner: Covert countermeasures disrupt deception detection by functional magnetic resonance imaging,” *Neuroimage,* vol. 55, no. 1, pp. 312-319, 2011.

[81] J. Hahm, H. K. Ji, J. Y. Jeong *et al.*, “Detection of Concealed Information: Combining a Virtual Mock Crime with a P300-based Guilty Knowledge Test,” *Cyberpsychology & Behavior,* vol. 12, no. 3, pp. 269-275, 2009.

[82] D. D. Langleben, L. Schroeder, J. A. Maldjian *et al.*, “Brain activity during simulated deception: An event-related functional magnetic resonance study,” *Neuroimage,* vol. 15, no. 3, pp. 727-732, Mar, 2002.

[83] M. Schneider, B. Varcuti, A. A. Karim *et al.*, “Neuroimaging of Deception in a Free-Choice Guilty Knowledge Test (GKT) after a Mock Crime Scenario,” *Psychophysiology,* vol. 46, no. 1, pp. S75-S75, Sep, 2009.

[84] A. R. Hevner, S. T. March, J. Park *et al.*, “Design Science in Information Systems Research,” *MIS Quarterly,* vol. 28, no. 1, pp. 75-105, 2004.