High-tech lie detection

By Stephanie Kanowitz | Jun 08, 2018

Technology has come a long way since the polygraph test was invented in the early 20th century. Advances have reshaped how researchers use lie-detector tests, and the most recent applications have gone digital.

Today, lie-detection techniques incorporate artificial intelligence, machine learning, analytics and biosensors that don't even have to touch the subject in question to get a reading. Whereas polygraph results are met with some doubt, these new tech-heavy techniques are more reliable, experts say, with accuracy passing human ability.

Whether they're kiosk screens, mouse-movement trackers or eye-movement monitors, lie-detection technology is taking advantage of all the Information Age has to offer. Here, we look at few examples.

AVATAR at the border

The Department of Homeland Security funded research of a virtual border agent called the Automated Virtual Agent for Truth Assessments in Real-Time about six years ago and did some light testing. Besides assessing the truthfulness of border crossers, AVATAR could be applied to processing applications for citizenship, asylum and refugee status, and reducing backlogs.

The technology uses AI, sensors and biometrics to flag individuals based on eye movements or changes in voice, posture and facial gestures. Users face a screen on a kiosk and talk to a virtual agent or the kiosk, which has sensors that note changes.

"The suite of tested sensors measure the individual's vocalics, kinesics, eye gaze, facial features, and pupil dilation to assess credibility," according to DHS. "Unlike human screeners who can become fatigued or distracted, the AVATAR is designed to maintain consistent vigilance to allow human agents to focus on high-risk travelers and facilitate the flow of legitimate trade and travel."

AVATAR has a success rate of 60 percent to 75 percent, Aaron Elkins, an AVATAR developer and assistant professor at San Diego University, told CNBC last month.

"Generally, the accuracy of humans as judges is about 54 to 60 percent at the most," he said. "And that's at our best days. We're not consistent."

In 2012, DHS tested AVATAR in Nogales, Ariz., where it interviewed volunteer travelers in the Trusted Traveler Program. Canada and the European Union have also tested it.

Telling reaction time

A group of Italian researchers, meanwhile, are studying whether the way a person moves a computer mouse could be used for lie detection. The idea is rooted in the fact that when people lie, they respond more slowly, according to the study. To that end, the researchers examined reaction-time-based memory. The technology, offered by Converus, is called IdentityDetect.

"The use of a mouse for recording responses has a number of advantages over the use of a keyboard," the paper states. "While the press of a button may permit only [reaction times] to be recorded, mouse recording allows several indicators to be collected, including but not limited to RT (e.g., velocity, acceleration, and trajectory)."

The researchers tested their theory by separating 40 subjects into two groups and asking them to answer questions about their identity -- name, birthdate and place of birth, for example -- using an online form. They told one group to tell the truth and the other to lie, using fake information the researchers provided. They also added unexpected questions such as "Is Florence the capital of your region of birth?" These unanticipated questions led respondents in the lying group to take longer to respond as they thought about their fake identities. The point was to detect such hesitation, and the researchers did.

"Unexpected questions may be embedded into an identity verification test to permit the identification of deceptive subjects with high accuracy," the researchers found. "Liars find it hard to respond to unexpected questions quickly and without errors. Their uncertainty is captured by mouse dynamics, as their motor behavior diverges from the ideal truth-teller trajectory."

Lyin' eyes

Three congressional candidates from California passed a lie-detector test designed for political candidates, according to a Converus release. The company's EyeDetect technology can detect deception in 30 minutes by analyzing involuntary eye behavior, such as pupil dilation and blink rate.

Test questions included queries about the illegal use of campaign funds, bribery and ties to terrorist organizations. At the end, the responses and measurements were uploaded to a cloud server, where algorithms determined whether the interviewee was truthful.

"Unlike polygraph, there are no cables or sensors attached to the examinee during an EyeDetect test," according to the release. "Because the true/false test is automated, and the results are determined by a computer algorithm, Converus says an EyeDetect test administrator cannot manipulate the outcome of the test or show bias -- which gives all examinees a consistent experience."

Fradulent fibbers

Ten police forces in the Spanish cities of Murcia and Malaga cracked down on insurance fraud a year ago by analyzing statements self-proclaimed victims gave to officers about robberies. An algorithm in the software helped officers identify false claimants. The tool was so successful -- detecting 31 and 49 offenses in the two regions, respectively, in one week -- that it's being implemented nationally, according to the journal Nature.

"In this case, the algorithm flagged up suspicious wording (based on a training set of statements known to be true and false), and left it up to the police to question suspects and get them to confess," the article stated. "A person, not a computer, made the final decision."

About the Author

Stephanie Kanowitz is a freelance writer based in northern Virginia.