

Publication: Brainstorm - Inside
Title: The business of biometrics
Publish date: 01 Jul 2023
Page: 50

Reach: 9235
AVE:R 27422.74
Author: Joanne Carew

Marco Wagner (left) and Gur Geva are adding liveness to facial recognition.

The copyright act of 1978 (as amended) prohibits the reproduction of this copy IN ANY FORMAT, without prior permission of the original publisher.

market iq



Publication: Brainstorm - Inside
Title: The business of biometrics
Publish date: 01 Jul 2023
Page: 51

Reach: 9235
AVE:R 27422.74
Author: Joanne Carew

The business of biometrics

The team at iiDENTIFii is looking to eliminate fraud by adding an additional layer of protection to its biometrics solution.

By **Joanne Carew**

Back in 2017, Marco Wagner and Gur Geva didn't really know each other. At the time, Wagner was the owner of a development consultancy and Geva was a chartered accountant. What brought them together was a big, hairy, audacious goal – a goal so compelling and so ballsy that it inspired the pair to take action.

"When Gur approached me, he told me we had to come up with a way to use a mobile device to stop identity fraud in South Africa and across Africa," says Wagner, co-founder and CTO at iiDENTIFii. "During our journey to find a solution to this problem, we've both had moments where we thought the other was totally insane, but you need to be a little insane to take on a problem as big as this."

Identity theft is one of the fastest growing crimes in the world. In fact, experts believe that someone's identity is stolen somewhere in the world every two seconds, says Geva, co-founder and CEO. As digitisation accelerates across Africa, the demand for "liveness" detection and online identity authentication services has become critical. The former is where iiDENTIFii really differentiates itself.

It's alive

In biometrics, liveness detection refers to a system's capacity to determine whether a fingerprint, face or any other biometric is genuine – taken from a live individual present at the time of capture – or not. This is needed to prevent criminals and impostors from tricking biometric systems using photographs, videos, masks or any other form of non-living artifact. "Our technology is a bit like a Lego piece that fits inside other people's applications, like a mobile application, a web application or website. So we don't develop mobile applications. We don't develop websites. These little Lego pieces have extremely powerful functionality in them and liveness detection is one example of this functionality; we supply two types of liveness detection – 3D and 4D detection," says Wagner.

He explains that their "Mercedes-Benz S-Class technology" also uses the dimension of time to guard against fraud. "We don't ask people to wink or blink or anything like that to prove that they are alive. Rather, we generate a unique sequence of lights on our servers in the cloud and then we send it down to the customer's device," he continues. This particular sequence is unique to a specific transaction. It is flashed on the user's face and a recording of how the light bounces off the user's face is analysed to assess if the person is three-dimensional and if they were actually "present" at the time of the transaction. "We've also integrated with the Department of Home Affairs and are able to further verify that someone is who they say they are by comparing our liveness detection data with the image printed on someone's ID document."

Describing how its digital identity solution works in practice, he says there's the potential for it to be used in the public sector to streamline things like border management and to improve election efficiency. "Because our solution aids authenticity, in an election scenario, it would eliminate human error and protect against duplicate votes. It would also eradicate the need for people to stand in long queues to cast their ballot because people would be able to vote via the web browser on their laptop or phone."

For Wagner, making sure that citizens and customers feel comfortable using these systems and trust that they're safe is essential in laying the foundations for a future where all digital transactions are secured using biometric solutions. "You build trust by letting people use these technologies on a daily basis. So, to give you an example, as smartphones have evolved, people have started using on-device biometrics more and more. You're using a fingerprint or facial recognition to unlock your phone or to access your banking app." But it takes time, he admits. "If you start talking about liveness detection, most people don't know what you're talking about. This tells us that there is a gap in the market and it's going to take time for us to fill it. But we are definitely making strides in the right direction."

AN AFRICAN SOLUTION FOR AFRICAN FACES

It's common for facial-recognition systems to misidentify people of colour more often than white people. The algorithm powering iiDENTIFii's enterprise-grade face authentication platform is trained on over 50 million faces in Africa, encompassing data from thousands of unique ethnicities and skin tones across the continent. "The African market is relatively untapped in terms of Identity Verification (IDV), especially from an enterprise-grade perspective," says iiDENTIFii's Gur Geva. While he admits that are a few smaller companies that are involved in IDV in Africa, few can do it at the scale needed to really make an impact across the continent. This needs to change.

www.marketiq.co.za | Tel: 011 884 7847 | enquiries@marketiq.co.za
The copyright act of 1978 (as amended) prohibits the reproduction of this copy IN ANY FORMAT, without prior permission of the original publisher.