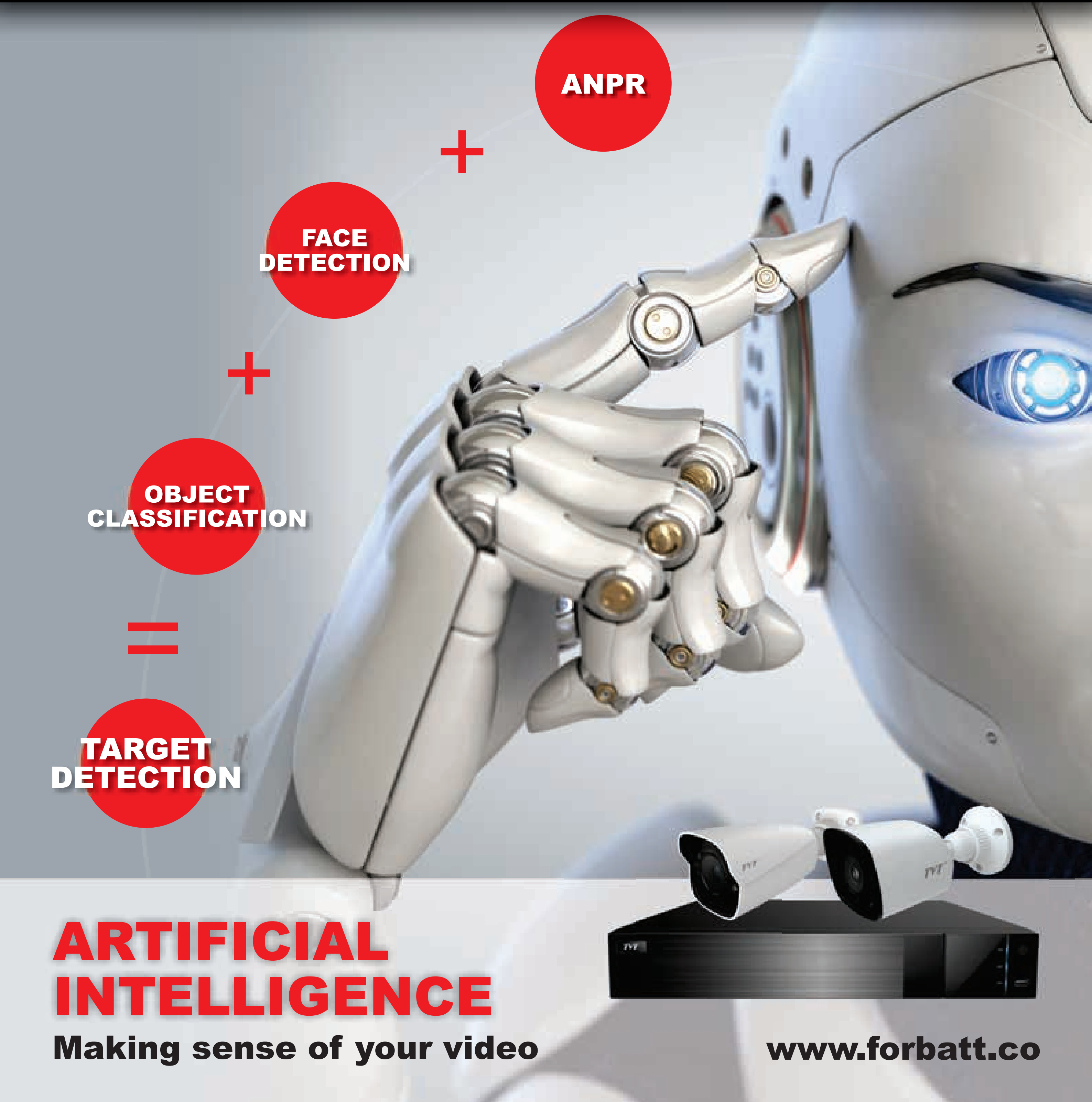
hi-tech SECURITY solutions

VOLUME 26 | ISSUE 3 **2020**

The authoritative resource for physical and converged security



Left to right: Walter Rautenbach, Hendrik Combrinck, Marco Wagener, Deon Janse Van Rensburg, Eric Chen.

Secure identification and authentication

By Andrew Seldon.

Hi-Tech Security Solutions hosted a round-table specifically to look at what is happening in the world of secure identity verification and authentication.

Whether it is via phishing or more traditional means, identity theft is a crime that plagues everyone, rich and poor. The seeming ease of stealing an identity has led to many considering and reconsidering the issues of identity verification and authentication, whether you are signing into social media, trying to retain some privacy online, accessing your bank account or coming in the door.

Hi-Tech Security Solutions hosted a round-table specifically to look at what is happening in the world of identity verification and authentication. Our goal was to cover the basics of what exactly verification and authentication are and to look at identity technologies and solutions that are fit for the financial industry, but to also cover a broader spectrum including other digital and physical access control requirements.

(It should be noted that the round-table took place before the COVID-19 'State of Disaster' was declared. – Ed.)

For the round-table, we had five guests on site, one connected via conference call, and one who couldn't make it and sent through written answers to a few questions we had. The on-site guests were:

- **Eric Chen:** senior solutions engineer from Dahua Technologies. Dahua has been in the CCTV space for more than 20 years and it has used its experience to move into the facial recognition market of late, and has been involved in safe city initiatives in various countries.
- **Hendrik Combrinck:** chief executive officer of ZKTeco. ZKTeco has been in the biometric market for over 20 years and has more recently moved into areas such as national identities where authentication and verification are critical.
- **Deon Janse Van Rensburg:** Africa manager for ViRDI Tech. ViRDI has been in South Africa for around 15 years and has been focused more on access control and human management systems and solutions, boasting the largest biometric footprint for a single client in Africa.
- **Walter Rautenbach:** managing director of neaMetrics (the Suprema distributor in SA). neaMetrics has been involved in identity verification projects since 2004, including the Home Affairs conversion of identity records to digital format (i.e., biometrics) as well as the Afiswitch criminal clearance solution and more.
- **Marco Wagener:** is from iiDENTIFii, a fairly new South African company that specialises in remote or mobile identity verification technologies that have been adopted by many banks in the country. The technology not only verifies people's identities remotely via facial recognition, but also recognises the official South African identity documents in the process. (Read more at https://www.securitysa.com/9181r.)
- **Gur Geva:** also from iiDENTIFii, joined via conference call. **Nicolas Garcia** from IDEMIA was unable to make the round-table and he submitted answers in writing, which we include on page 22.

Starting at the beginning

Most, if not all readers will have come across biometric identification technologies in businesses where they are used for access control or time and attendance functions, among others; many will also have seen banks using fingerprint verification to identify people by cross referencing their fingerprint biometrics with Home Affairs. In addition, there are few readers which will not have come across and used biometric authentication, either fingerprint or facial, on today's mobile devices.

But there is a difference when talking about using biometrics at the door and giving them access to a building, as compared to using it in a bank to authorise transactions, or in government to get a new passport. Our first question to the round-table was to highlight the difference between authenticating a user and verifying them. And, of course, with 'touchless' facial recognition apparently a good solution in light of the coronavirus, how different are authentication and verification from 'recognition'?

Janse van Rensburg explains that from a ViRDI perspective, verifying a person's identity usually involves multi-factor authentication, such as a card and biometrics, or a PIN and biometrics, and then comparing the data input with one individual record on the database. In other words, the individual claims to be someone and that person's existing data is compared to the data provided at the terminal or access point.

Identifying a person, on the other hand, usually relies on single-factor authentication, such as a biometric. The data collected is then compared to a database of identities and an individual is matched to one of the entries in the database.

Wagener adds that iiDENTIFii associates identification with the initial enrolment process of an individual. This relies on multi-factor authentication, starting normally with a biometric taken on a mobile device (facial or fingerprint) along with their identity documents (which are sent from the mobile or remote device). This information is compared to the Home Affairs database and associated to a specific account, a one-to-one verification process. When the person returns and wants to transact on the account, they are then authenticated, proving they are the identity that was enrolled.

Combrinck echoes this, noting that verification must be conducted with some form of proof that was given to the person by a trusted authority – such as an ID card, driver's licence or passport – and the identity is then saved to a database. Following that, other tokens or certifications are created to allow the person to be authenticated and authorised on other systems.

Geva adds that, looking at facial biometrics, recognition is picking a face out of a crowd and matching it to a database. This is often done in safe city environments and can be used to pick up someone jaywalking, for example. Verification is actually done with the consent of the individual and with proof they provide of their identity to ensure that their data is accurate and they are who they say they are.

Rautenbach explains that the verification process is 'confirming'. Making use of additional data, such as an ID card, the person is confirmed to be a specific individual. From there the individual is issued with a specific token (a password to log into the office computer, a biometric to come in the door or authorise a transaction, etc.), which they can use to authenticate themselves on a regular basis. Linking the token to other systems then allows you to secure the 'identity chain'. He notes that while this works in South Africa with a central source of identity (Home Affairs), it becomes more complicated in countries where this source does not exist.

There can be no authentication if there is no reliable and trusted database to work from, adds Chen. He gives the example that a bank could verify you against Home Affairs and then in future authenticate you to their own database which they create and include your biometrics in after Home Affairs confirms you are who you claim to be. (Of course, they should tell people they are saving their biometrics and not only verifying their identity with the Home Affairs database.)

The identity chain

Of course, there is always a chance that a company can be conned into believing that someone is someone else because they have faked their identity and are making use of a 'clean' identity, or because they have 'contacts' in various government departments that can hide the truth. This is why, according to Rautenbach, the idea of an identity chain is so important.

The identity chain concept is a means of capturing someone's identity and following it 'from cradle to grave', by initially capturing accurate identity information and then continuously updating the information throughout the life of the person. An accurate chain will allow organisations to know that someone is who they claim to be with confidence because they have a history of 'being' that person. It will stop identities from appearing out of nowhere when an unregistered adult decides to register without any previous records (as happened and still happens in South Africa).

On a smaller scale, facial recognition can create an identity chain in various environments. In an airport, for example, facial recognition can recognise a face as it enters the airport. This is merely a process of recognition, in other words, mapping the unique features of a face and storing the information anonymously. If one adds analytics to the process, the information can be supplemented with metadata such as age range, gender, race, and in the near future gait recognition.

At a later stage, the person can be properly identified when they are at a check-in counter and hand over their identity documents. In the meanwhile, the airport can, either actively or historically (in the event of an incident), identify where and when this individual went while on the premises. And in the event of a crime or act of terrorism, who they met with and what they did can also be determined. The ideal is to have all this done in real time by the analytics system, not to spy on people, but to try and proactively identify suspicious behaviour and prevent incidents.

Of course, this depends on where one is. In China or Dubai, this type of identity chain is standard procedure. Janse Van Rensburg notes that Dubai uses multiple biometric modalities to identify people from the moment they arrive. By the time you leave the airport, the authorities can find you or identify you almost anywhere.

In Europe, this is becoming a problem, he says, because of the GDPR (General Data Protection Regulation) regulations that are limiting the use of biometrics dramatically, especially facial biometrics – but the law applies to any type of personally identifiable information. The frightening thing is that there is scope for individuals or EU organisations to sue biometric suppliers and installers if someone complains about a breach of privacy under the GDPR. What will happen in a year or two in South Africa when PoPIA (Protection of Personal Information Act) gains some teeth remains to be seen.

Interestingly, the countries where biometrics are used most effectively today are third world and formerly third world countries. India rolled out its Aadhaar programme to create official identities for a billion people, and associates government payments such as pensions, etc. with this system. China's move to using facial biometrics is well-known and causing concern in some quarters. And Africa and South America are also seeing increased use and rollouts of biometrics in many countries.

Of course, privacy legislation and biometric identification is all good and well, but as Wagener says, it all depends on the enforcement of regulations. The best regulations and identification technologies are useless if not backed by competent and secure management and enforcement.

In Africa, Combrinck adds, the ID4Africa initiative is growing and creating success stories in many locations. The programme is focused on creating identities for everyone in Africa, but specifically allocating an identity to every person that is born. Without that identity, people may not be able to get a SIM card, or bank account or even go to school.

Officially, "The ID4Africa Movement is driven by the need to establish identity-for-all, not just as a legal right, but also as a practical necessity to enable inclusive access to services in Africa." (Find out more at www.id4africa.com)

However, it's more than simply a face or a fingerprint. Wagener says iiDENTIFii realised this when developing its solution. While the method of identification needs to be reliable and secure (such as facial recognition), more important in instances of remote verification and authentication is proof of presence and proof of life. Dealing with fake pictures and videos, as well as the seemingly never-ending onslaught of cyber fraud, must be part of developing and expanding the identity chain.

Deon Janse Van Rensburg.

Hendrik Combrinck.

Eric Chen.

Fingerprints still the first choice

While we constantly hear about new forms of biometric identification, whether it's facial, ear, gait or even DNA, the fact is that fingerprints are and will remain the primary biometric for identification for some time. Rautenbach explains that is due to the historical research and use of fingerprints before technology was able to read a fingerprint, as well as the criminal aspect – criminal identification relies on fingerprints.

The challenge with fingerprints is that there has to be a specific device on the ground at the point of identification (and which people have to touch, which can make people nervous in the era of COVID-19). Facial biometrics are easier to capture from a distance, but there are also challenges in terms of lighting, 3D masking and liveness detection, etc. The fact is that for each security measure developed, criminals develop a new way around it. However, he says facial biometrics will increase over time, but whether we will see it replacing fingerprints completely is unlikely (not for a long time, anyway).

Chen adds to the debate, noting that fingerprints are still more accurate as an identification medium than facial – although facial biometrics have improved tremendously. Facial works on a smartphone, for example, because the user holds the phone close to their face and the software is able to get a clear, face-on image. In other environments, like a safe city for example, cameras may be installed at a particular angle and not always get a direct image of a face, and there are constantly changing lighting conditions to be aware of.

Possibly the most important benefit of fingerprint identification currently is the cost, Chen notes. Although the cost of facial recognition systems has declined rapidly, it is still far more costly than fingerprint systems. Moreover, infrastructure is also an issue as fingerprint biometrics send small bits of information to a server for verification, while facial systems need far more bandwidth. Hence, Chen also believes fingerprints will be the primary identification mechanism for a long time, especially in Africa where the infrastructure challenges abound.

Wagener also notes that trust in facial recognition is still something that has to find a broad foothold. This, adds Geva, was a challenge the company had to overcome when it launched its solution; in other words, trust that facial identification was reliable in a remote context where the person was not present (at a bank, for example) and the hardware through which the identification process was handled was also not present or even in the control or the organisation.

The security of facial recognition

Of course, with more facial recognition products becoming available at more reasonable costs, and with the COVID-19 pandemic, the no-touch aspect of facial biometrics is becoming a more popular option. However, as noted, the trust aspect is an issue with many believing that a picture or 3D mask, or a fake AI-generated video will be able to fool a facial scanner.

Rautenbach explains that the process of facial recognition can be divided into two areas. The traditional method was visual verification where the image of the person was captured and analysed. This is naturally open to fraud and so vendors have developed additional ways of recognising faces that don't rely only on the image of a face.

Suprema, for example, uses Infrared (IR) and 3D technologies (among others) to analyse a face, making it impossible to simply show a picture or video to the reader and be verified. Other companies have done the same. The problem is that when one wants to run your visitor management on facial recognition, this can be a problem if the visitor sends a picture of their face to the company – this is why facial recognition in general will consist of a hybrid process of comparing pictures as well as other technology like IR.

ZKTeco made the decision to use visible light facial recognition for its facial recognition products to allow for recognition at a greater distance. Combrinck says this allows its products to be used in multiple environments for recognition and authentication – such as greeting a returning VIP customer. For more secure verification, ZKTeco uses a combination of visible and IR light in the same device to more accurately identify the individual. For example, in an access control setting, the approaching individual is scanned with visible light as they approach and when they are closer to the reader, Infrared is used for more accurate analysis and identification before access is granted.

Janse Van Rensburg adds that ViRDI's facial recognition launched using IR for recognition because they realised the inadequacy of visible light systems in accurate and reliable identification. However, the company has also realised that there is a place for visible light in their solutions and will release new hybrid products in the near future. This will make visitor management, for example, easier as visitors using their new system will be able to enrol via an app or Web page with their image (or selfie) before arriving to speed the process once they arrive.

Geva adds that liveness and presence is also a challenge in facial recognition, especially when doing remote verification. In the past, asking a person to move or simply looking at the image and seeing the natural movements of a person, such as blinking, were seen as acceptable liveness and presence verifiers. Today, however, cheap software is available online that can create 'virtual puppets' that can mimic humans movements accurately.

Continued on page 20

Walter Rautenbach.

Marco Wagener.

Gur Geva.

Continued from page 18

This was a significant challenge in remote verification for iiDENTIFii as the company wanted to roll its products out across Africa, where many people would be using older phones without IR and other capabilities. The solution was to use different colours of light reflection, a process that works on older phones.

Wagener adds the company only uses the user's device as a proxy to capture data and flash different lighting onto his/her face. Assuming that every device is compromised, the main processing is done on the server to enhance the security of the process as a whole and to cater for older cameras – a 2 MP VGA camera is sufficient for iiDENTIFii's needs.

Chen makes a good point that the technology used also depends on the situation and the environment. Visible light recognition would be good enough for identifying customers, but not for allowing them into restricted areas. In this instance, IR would be required. For recognition outside, again in a safe city concept or perhaps in environments like airports, visible light is the only option and should be supported by other technologies for more accurate identification. With technology like WDR (wide dynamic range), surveillance cameras can always adapt to different lighting conditions.

Combrinck notes that ZKTeco has WDR built into its devices. In addition, its algorithm continually updates its identity templates the more a person uses it, creating more accurate templates over time. Janse Van Rensburg agrees, saying it is a "learning process", both in terms of improving the facial templates as well as improving the hardware and software in devices over time.

Biometrics going forward

Looking at the biometric identification market over the next few years, Hi-Tech Security Solutions asked the round-table attendees to wrap up by highlighting what they see happening in their segments of the market in terms of where the market is going and what customers will be wanting from their suppliers.

Combrinck says ZKTeco is focusing on visible light facial recognition technologies because it sees traditional fingerprint readers disappearing over time in favour of facial recognition. And he notes that facial recognition won't only be done on specific devices, but will also form part of surveillance cameras over time, reducing the amount of security technology needed without compromising functionality. Moreover, ZKTeco sees multimodal biometrics becoming more important to give users options.

For Dahua, Chen says the focus has always been on security, but the company is seeing opportunities and demand to use facial recognition devices for business operations, such as understanding which customers are frequenting retail stores to allow the retailer to better tailor marketing and store layout for the demographic that will be there at specific times. Therefore, the company is looking at expanding from security into providing more business intelligence from its devices to drive customer revenue.

Wagener says iiDENTIFii is focusing on the Web. People are getting more apathetic to installing yet another app on their phone and so the company is looking at more Web integration to offer its product via a browser for easier verification and authentication, and we can expect to see the solution 'branch out' to incorporate more functionality such as easier online transactions.

From a Suprema perspective, Rautenbach says the company will continue delivering fingerprint and facial biometric products, and it will continue enhancing BioSign, Suprema's packaged algorithms which assist prominent manufactures by securing millions of mobile devices, an area it believes will remain in a rapid growth trend for many years. He adds that the need for multi-factor and multi-modal authentication will continue receiving more and more attention in the drive for higher security, accuracy and availability. Looking beyond the traditional fingerprint and facial biometric world, Rautenbach believes in incorporating all modalities, including voice and behaviour, when building multimodal ensembles, as these can play a key role in the African identity landscape.

ViRDI has put a lot of focus on touchless technologies for authentication as it, as all the other attendees, believes that the 'device against the wall' will not have a very long lifespan. In addition, Janse Van Rensburg says the integration to mobile authentication is also receiving attention, for example for those places where shopping without paying will become the norm – such as the Amazon Go shopping experience (see more at https://www.youtube.com/watch?v=NrmMk1Myrxc). Although this business model may not be seen in South Africa very soon.

For more information contact:

- Dahua Technology South Africa, +27 10 593 3242, sales.za@dahuatech.com, www.dahuasecurity.com/sa
- iiDENTIFii, +27 21 286 9104, info@iidentifii.com, www.iidentifii.com
- neaMetrics, 0861 632 638, info@neametrics.com, www.neametrics.com
- ViRDI Tech, +27 11 454 6006, deon@virditech.co.za, www.virditech.co.za
- ZKTeco (SA), +27 12 259 1047, sales@zkteco.co.za, www.zkteco.co.za