EAB Newsletter July 1, 2018

Next events:

September 24 – 25, 2018: EAB Research Projects Conference (EAB–RPC) 2018

September 25, 2018: 8th EAB General Assembly

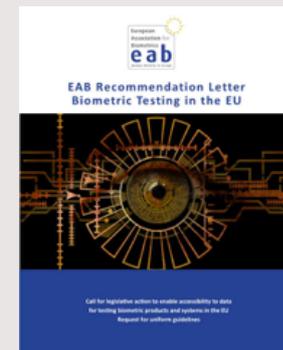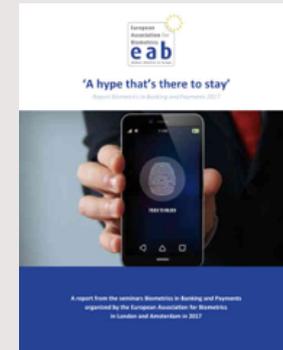**September 26, 2018:** German TeleTrusT Biometrics Working Group

September 26, 2018: EAB Biometrics Research and Industry Awards 2018

September 27 – 28, 2018: BIOSIG 2018 – 17th International Conference of the Biometrics Special Interest Group

November 9, 2018: Seminar on Biometric Data and the GDPR

November 23, 2018: Norsk Biometri Forum Meeting

Appointment of CEO

The European Association for Biometrics (EAB) today announced the appointment of Michiel van der Veen as Chief Executive Officer.

Full story

EAB Banking Seminars 2018

Where biometrics meets FinTech:

Join us for this years EAB Banking Seminars to debate one of the biggest questions facing FinTech and online services – "Do you REALLY know your customers?"

Full story

Draft European Regulation on Identity Cards

The European Commission has published a draft regulation on on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens.

Full story

Special reports:

Table of contents

Appointment of CEO

The European Association for Biometrics (EAB) today announced the appointment of Michiel van der Veen as Chief Executive Officer.

EAB's Chairman Alexander Nouak said, "The appointment of Michiel as CEO signals a new chapter in the EAB movement and our drive to be the leading association for biometrics and identity in Europe."

Michiel van der Veen said, "I'm honoured to be appointed CEO of the EAB. The association is fast becoming a leading forum for industry, governments and academia to network and share trends about biometrics and digital identity." Michiel adds, "Our focus will be to continue to raise the profile and reputation of the EAB as we expand further across Europe and to deliver even better value to our members, leveraging the strength of our network."

The appointment comes at a time when biometrics and digital identity are increasingly a part of everyday life for Europe's 750 million citizens. According to Michiel van der Veen, "In recent years, the EAB membership has grown to include almost every sector, f rom border protection, eHealth to financial services. Our job is to offer them impartial advice as they navigate a wide range of issues, from regulatory frameworks to new technologies."

About Michiel van der Veen: He is an experienced executive and well known expert in the field of biometrics and digital identity. After a career at Philips Electronics, Michiel founded priv–ID, an early innovator in biometric and digital identity. It later merged with GenKey in 2011, with Michiel appointed CEO. Michiel led GenKey through multiple stages of growth to become one of the most trusted brands in the market, providing Identity for Development. Michiel is also a regular industry contributor on digital identity and biometrics, along with future thinking about innovation and market trends. Michiel has a Ph.D from the Swiss Federal Institute of Technology (ETH Zurich) and further business education from Stanford.

EAB Banking Seminars 2018

London, Frankfurt, Amsterdam, Madrid

Where biometrics meets FinTech:

Join us for this years EAB Banking Seminars to debate one of the biggest questions facing FinTech and online services – "Do you REALLY know your customers?"

Seminars are attended by the financial sector and ID industry and will take place between September and December 2018 in Europe's financial capitals – London, Frankfurt, Amsterdam and Madrid. We will discuss the latest trends that are helping to improve customer ID security, such as blockchain, AI and smartphone biometrics; share best practice models; and assess the impact of new legislation, like GDPR. Entries are now open for biometrics and ID vendors to attend, share insights and demonstrate new product releases to a targeted audience from the financial sector.

Please contact the event chair, Michiel van der Veen, for more information.

Contact: Event chair:

Michiel van der Veen
email: banking_seminar@eab.org
Tel: +31 6 10392077

Draft European Regulation on Identity Cards

The European Commission has published a draft regulation on on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens.

The context of the proposal is that ensuring the security of travel and identity documents is a key element in the fight against terrorism and organised crime and building genuine Security Union.

Of twenty-six EU Member States that issue identity cards to their nationals, identity card ownership is common and compulsory in 15 Member States. Currently, security levels of national ID and of residence documents vary significantly, which increases the risk of falsification and document fraud.

According to the proposed draft regulation, fingerprint reference in ID-Cards will become mandatory and the specification will be aligned to ICAO 9303. Moreover the document indicates a five-year phasing out period of previous formats.

You can read the full draft document at: https://ec.europa.eu/info/sites/info/files/placeholder_1.pdf

Report on the Rise of Biometric Cards

Must read for the industry
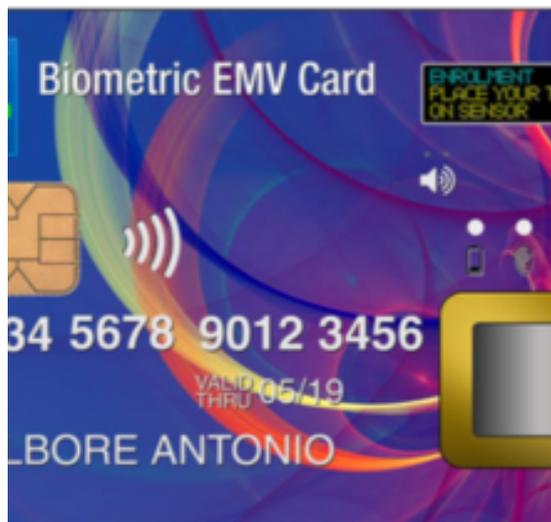
Embedded security news (Antonio D'Albore) released the world first independent research on biometric smart cards. Biometric smart cards are being adopted across markets with recent deployments in the payment industry by VISA and Mastercard.

The report gives a comprehensive overview of the underlying technology, the value chain and the relevant suppliers and stakeholders. The report further provides a vision for the future trends like liveness detection, PCB design simplification and miniaturization, behavioral biometrics, contactless fingerprints, DNA biometrics or vein biometrics.

A download is available here:

https://embeddedsecuritynews.com/wp-content/uploads/2018/06/2018-06-the_rise_of_biometric_cards.pdf

Framework to Evaluate Unlinkability in Biometric Template Protection Systems
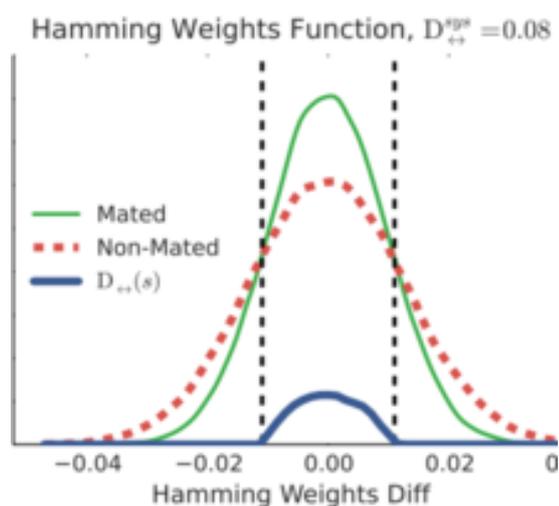
The discussion on the GDPR has raised privacy concerns regarding the storage and use of biometric data. While the international standard ISO/IEC 24745 has established two main requirements for protecting biometric templates i) irreversibility and ii) unlinkability back in 2011, only recently a framework to evaluate unlinkability is presented.

Numerous efforts have been directed to the development and analysis of irreversible templates. However, there is still no systematic quantitative manner to analyse the unlinkability of such templates. In a recent work of the dasec-research group this shortcoming is address by proposing a new general framework for the evaluation of biometric templates' unlinkability. To illustrate the potential of the approach, it is applied to assess the unlinkability of four state-of-the-art techniques for biometric template protection: biometric salting, Bloom filters, Homomorphic Encryption and block re-mapping.

You can read more details at:

https://dasec.h-da.de/wp-content/uploads/2018/06/2018_UnlinkabilityMetric_techReport.pdf

Seminar on biometric data and the GDPR

9 November 2018

The Center for Information Technology and Intellectual Property rights (CITIP) of the KU Leuven and the University of Kent together with the EAB are organizing a seminar on biometric data use in the new era of the GDPR.

Both academic points of view and practical application in various sectors will be discussed. The event will take place in 3000 Leuven, Sint-Michielsstraat 6, a 20 min. train ride from Brussels. Save the date. The programme will follow soon.

If you are interested in more details of the seminar please contact: els.kindt@kuleuven.be

EAB welcomes new Newsletter Editor

Javier Galbally joined the editorial Team of the EAB Newsletter
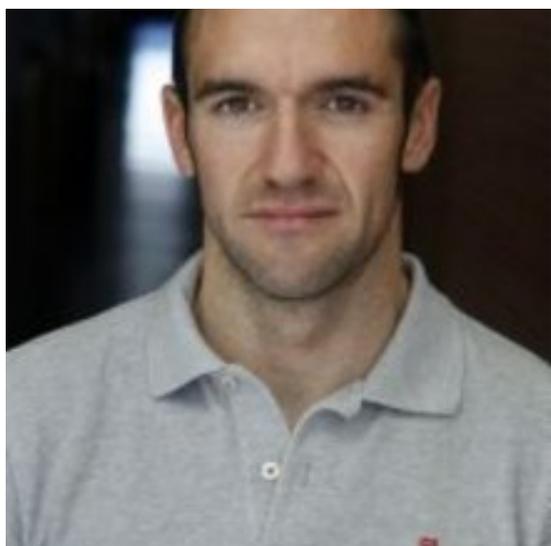
The EAB is pleased to announce Javier Galbally as new editorial member of the EAB newsletter! Javier Galbally received the M.Sc. degree in Electrical Engineering from the Universidad de Cantabria, Santander, Spain, in 2005, and the Ph.D. degree in Electrical Engineering from the Universidad Autónoma de Madrid, Madrid, Spain, in 2009. In 2013, he joined the DG Joint Research Centre, European Commission, where he is currently a Post-Doctoral Researcher. His research interests are mainly focused on pattern and biometric recognition. He has co-authored over 100 biometric-related publications and is the current Scientific Chair of the EAB Research Projects Conference.

Now the EAB Newsletter will be sent out more frequently. The newsletter will be displayed into your email browser, including Outlook. The events calender will be included, showing the upcoming EAB activities. A special section presents reports from EAB events or other documents that are in the interest of our community.

All EAB members are invited to submit content for the newsletter. This can be about achievements in research and development, new projects in the area of biometrics and idientity in Europe and abroad, developments in EU policy making, projects on national ID, health care or financial services etc. For each newsletter the editors Christoph Busch, Christain Rathgeb and Javier Galbally will compose a new set of articles and other content. For any suggestions you can contact Christoph Busch at christoph.busch@h-da.de.

Forming a strong EU-research consortium and proposal

Halmstad University, the Swedish Biometrics Forum, and the European Association of Biometrics hosted a one-day workshop on 8th June near Copenhagen Airport with the purpose of discussing research ideas for a proposal to EU Horizon 2020 in the area of identification and security.

Eleven participants from different countries participated in the meeting, plus six more participants that could not attend but provided input prior to the meeting. In the first session, discussions started around the topic of continuous biometrics. Several calls for proposal with deadline on August 2019 were discussed, and existing EU projects in biometrics were also reviewed in order to find synergies, and also to avoid replicating ideas. The participants (divided into two working groups) then had a brainstorming session to identify suitable project ideas. There was also a presentation from a representative of the Swedish Innovation Agency (Vinnova), which is also the EU National Contact Point of Sweden. An executive summary and report of discussions will be circulated among participants of the meeting, with a follow-up meeting proposed to take place after the summer.

UK Biometrics Commissioner's annual report

The Biometrics Commissioner in the U.K. has published its fourth annual report. The position of Commissioner for the Retention and Use of Biometric Material was created by the Protection of Freedoms Act 2012 to provide assurance to the Home Secretary and to the U.K. Parliament on the working of that legislation. In addition, that legislation granted to the Biometrics Commissioner oversight and some limited decision making powers as regards the retention and use of biometrics (DNA samples, DNA profiles and fingerprints).

The report was published in June and covers casework activities, the general operation of the Protection of Freedoms Act 2012 regime and a variety of issues that have arisen in connection with its operation.

You can download the full report from:

https://www.gov.uk/government/news/biometrics-commissioners-fourth-annual-report-2017

Ottawa expands program to collect fingerprints, photos from foreign nationals coming to Canada

Privacy experts flag risks involved in collecting, storing and sharing sensitive personal information

Canada is expanding a program to collect biometric data — including fingerprints — from foreign nationals coming to this country, while experts are warning of the potential for heightened risks to privacy.

The expanded biometrics program will be rolled out over two years, beginning next month, with new requirements to collect biometric data from people from Europe, the Middle East and Africa coming to Canada to visit, work, study or immigrate. Previously, the program was limited to visa applicants from countries believed to pose a higher risk of immigration document fraud, as well as refugee claimants and asylum seekers.

Immigration Minister Ahmed Hussen has said the program's expansion from 30 to about 150 countries will strengthen border and immigration systems with the ability to quickly and accurately establish a traveller's identity.

Source

US to fingerprint child visa sponsors

The Trump administration has announced it plans to fingerprint parents claiming custody of children who entered the United States unaccompanied

Washington has said the move aims to prevent migrant children from going missing in the system, but that immigration advocates say it will discourage parents from claiming their children for fear of detention and deportation.

"We're going to more thoroughly vet sponsors," said Steven Wagner, acting assistant secretary of the Department of Health and Human Services' (HHS) Administration for Children and Families, in a telephone briefing with reporters. "With DHS' cooperation we will conduct a fingerprint-based background check on every sponsor."

HHS is ultimately responsible for finding housing for migrant children, and the Department of Homeland Security (DHS) enforces immigration policy. Under a new memorandum, DHS would help HHS fingerprint every individual claiming custody of a child, senior officials said.

Currently, parents are not required to submit fingerprints to obtain custody of their children. Under the new protocol, to be implemented in a few weeks, the Department of Homeland Security (DHS) will assist the Department of Health and Human Services (HHS) in fingerprinting every parent who claims custody.

Federal laws stipulate that unaccompanied immigrant children cannot be incarcerated. Instead, HHS houses them in federal shelters until the minors are placed with sponsors, typically close relatives such as parents or siblings.

Source

Digital Transformation in Airports Takes Off with Biometrics and Blockchain

Data monetization, product portfolio expansion, and diversification are key to exploiting emerging growth opportunities, finds Frost & Sullivan

Frost & Sullivan's recent analysis, Digital Transformation in Airports, reveals that increased passenger traffic and global capacity constraints will drive airport IT spending to $4.63 billion by 2023. Airports are developing their digital transformation roadmap in line with strategic planning activities to address key performance indicators across all areas of the airport operation.

Digital transformation in airports is creating growth opportunities across the globe with renewed commitment to infrastructure modernization and expansion creating a dynamic environment. In Europe, airports are motivated to invest in digitalizing operations due to physical infrastructure constraints, while Asia-Pacific airports are seen more open to innovation as a brand attribute and to enhance the airport experience. However, many airports endeavor to develop solutions in-house with local expertise and partnerships.

Technologies driving the digital transformation process in the airport environment include:

Biometrics: Biometrics applications focus on border control, reducing bottlenecks by automating processes. The technology is now being introduced across all touchpoints, in the form of identity management for self-service kiosks, aiming to create seamless passenger journeys. In the future passengers will be submitting biometric data (enrollment) at the first airport touchpoint and will only need to verify their identity in all subsequent originating airport touchpoints, with the possibly to further extend this facility at destination airport touchpoints.

Blockchain: Blockchain technology, as a trusted network for storing biometric and other personal data, can be used to create secure and faster passenger journeys. Blockchain could also prove to be the catalyst for a truly collaborative airport environment, among airport stakeholders that today work in silos. Passengers may be willing to share even more data about themselves, in exchange for valued personalized services and products, while blockchain eliminates any security or privacy concerns.

Analytics: The data generated by various airport systems are collated and analyzed to provide historic, real-time and forecasted data that will empower the operator to take proactive steps to deal with peak operational periods and disruptions.

Artificial Intelligence: Artificial Intelligence (AI) is already been used in narrow passenger-related applications, from chatbots to predicting preferences and recommending suitable products/services in the information and pre-travel stages of the passenger journey. It will be increasingly used in the e-commerce function of an airport, as well as in enabling operators to better manage airport spaces and allocating resources, according to optimized flow prediction models.

Source

Biometrics Could Be The Future Of mPOS

Tap to pay. Dip to pay. Smile to pay. Forget reinventing the payments wheel — it seems many innovators are looking to replace it

The PYMNTS Mobile Point of Sale (mPOS) tracker highlighted Singapore-based mPOS provider Touché for its fingerprint reader, which enables consumers who may have forgotten their phone or wallet at home to pay using something they can't forget: their finger. By touching the mPOS, the customer identifies themselves as the owner of linked payment cards and credentials.

CEO and Founder Sahba Saint-Claire told PYMNTS that fingerprint images are not stored. Instead, the fingerprint populates a template that is hashed and encrypted on Touché's database, and card information is tokenized. The device also only talks to their server, changing the encryption key each time the function is used. Saint-Claire said security could help contribute to wider adoption of biometric payment methods, which he believes are the future — but, "It takes some time for some people to feel comfortable," he said. "There will be a time lag."

Touché is far from the only one working on payment methods like this. Here are some of the other big industry names venturing into biometrics.

– Ingenico

– Samsung

– Mastercard

– Visa

– HBSC

[Source](#)

The future of facial recognition technology in theme parks and attractions

Biometric technology is at the forefront of leisure business innovation

Changing consumer expectations have, in particular, had a significant impact on theme parks and attractions where consumers are demanding more from their digital experiences, bigger and better thrills, and rides that reach the physical limits of possibility. As a result, theme parks and attractions are using innovative imaging technology to capture joyful moments and enhance the visitor experience in a non-intrusive way, encouraging organic sharing, loyalty and brand engagement.

Biometric technology is at the forefront of leisure business innovation. Facial recognition enables content created at a theme park or attraction to be identified and organized, seamlessly presenting visitors with their own personalized digital album. If they opt-in to facial recognition for their visit, then advanced association technology can identify them at multiple content creation points throughout, with no physical touchpoints or additional staffing necessary.

Visitors to the world's leading destinations can then select their image from an existing photo or selfie upload. Content-hungry consumers can be presented with the opportunity to immediately purchase images and videos, along with the option of sharing instantly on social media, or enjoying and sharing content post-visit.

Source

Researchers create photo filter that disables facial recognition

Neural net based constrained photo optimization

Professor Parham Aarabi and graduate student Avishek Bose are using "neural net based constrained optimization" to disrupt face detection software.

The University of Toronto researchers used existing knowledge of detection software that says "small, often imperceptible, perturbations can be added to images to fool a typical classification network into misclassifying them." Their dynamic "attack" algorithm "produc[es] small perturbations that, when added to an input face image, causes the pre-trained face detector to fail."

Aarabi and Bose designed two different, opposing neural networks — one that attempts to identify faces and the other that works to "disrupt" that identification — using 'adversarial training', a deep learning technique that puts two opposing AI algorithms in a sort of digital cage match.

Source

Native face authentication support coming to Android SDK

AOSP commit hints at native 'face authentication' support in Android alongside iris scanning
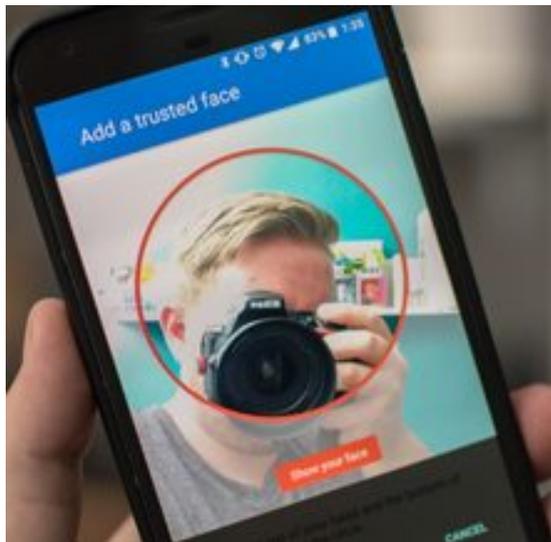
Back in March, we saw a third-party start work on adding official iris scanning functionality to the Android Open Source Project. Now, we've found code commits that hint at a more elaborate face recognition feature than the current Trusted Face Smart Lock.

The commit in AOSP is labeled as 'Add face authentication framework.' There isn't too much to gain from this commit just yet, but with this in place, manufacturers could call upon this API when it's implemented. This way, companies like OnePlus and others don't have to try to build their own.

Additionally, the commit states that unlike fingerprints, you can only register one face per user on the device. This is most likely to keep the processing power down, making it so the phone only has one template that it needs to compare your face to.

Interestingly enough, the primary person working on this feature is named Gilad Bretter and happens to work for Intel. It's not quite clear why Intel would be investing its employee's time to add such a feature to Android.

One thing to note is that this line of work has been in development since March. These new commits show continued work on the feature.

Source

Face, Iris and Pulse Biometrics Close in on Fingerprint Tech

Growing market share in Face, Iris and Pulse Biometric Technoogies

Face, iris and pulse-based biometric authentication systems will increasingly eat away at the market share of fingerprint technologies, according to a new report from ABI Research.

The analyst claimed in its Biometric Technologies and Applications report that the falling cost of iris recognition will spur uptake, while facial recognition continues to improve in accuracy thanks to advanced machine learning algorithms.

The latter has already seen significant increase in penetration thanks to Apple's decision to incorporate it into the iPhone X, while Samsung offers iris recognition in the Galaxy S8 and S9, the analyst continued.

The Internet of Things is also driving an uptake in newer biometric systems: with card-free ATMs being developed by Samsung and Diebold Nixdorf, OEMs in the automotive sector including GM, Nissan and Volvo investing heavily and new government rules in APAC set to mandate biometrics in a range of sectors including banking and telecoms, ABI Research claimed.

Source

Footsteps, Pressure Sensors, and AI: The Next Step in Airport Security

University of Machaster in collaboration with the University of Madrid providing a non-intrusive method of identity verification

Vision

Accelerometry
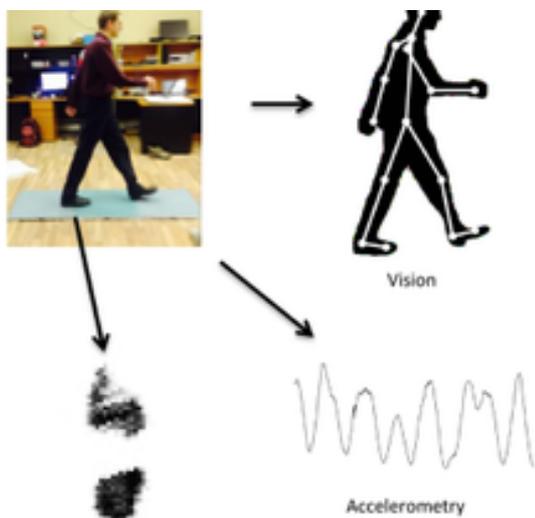
The University of Manchester's school of electrical and electronic engineering, in collaboration with the University of Madrid, has developed a behavioral biometric verification system that can measure a human's individual gait or walking pattern, enabling successful identification of a person simply as they walk on a pressure pad in the floor and analyzing the footstep's 3D and time-based data.

With this system, the researchers claim that the way a person walks and analysis of that individual's footsteps could be used as a biometric at airport security instead of fingerprinting and eye-scanning, providing a non-intrusive method of identity verification.

The results, published in a machine-learning research journal, the IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), earlier this year showed that, on average, the AI system developed correctly identified an individual almost 100% of the time, with just a 0.7% error rate.

Physical biometrics, such as fingerprints, facial recognition, and retinal scans, are currently more commonly used for security purposes. However, behavioral biometrics such as gait recognition can also capture unique signatures delivered by a person's natural behavioral and movement patterns. The team tested their data by using a large number of so-called "impostors" and a small number of users in three real-world security scenarios: airport security checkpoints, the workplace, and the home environment.

Source

Face Recognition is now being used in schools, but it won't stop mass shootings

School districts have purchased face recognition technology as part of a purported effort to prevent school shootings

Officials at the Lockport, New York, school district have purchased face recognition technology as part of a purported effort to prevent school shootings. Starting in September, all 10 of Lockport District's school buildings, just north of Buffalo, will be outfitted with a surveillance system that can identify faces and objects. The software, known as Aegis, was developed by SN Technologies Corp., a Canadian biometrics firm that specifically advertises to schools. It can be used to alert officials to whenever sex offenders, suspended students, fired employees, suspected gang members, or anyone else placed on a school's "blacklist" enters the premises. Aegis also sends alerts any time one of the "top 10" most popular guns used in school shootings appears in view of a camera.

The district is spending most of its recent $4 million state "Smart School" grant on these and other enhancements to its security systems, including bullet-proof greeter windows and a mass notification system, according to the Niagra Gazette. "We always have to be on our guard. We can't let our guard down," Lockport Superintendent Michelle T. Bradley told the Buffalo News. "For the Board of Education and the Lockport City School District, this is the No. 1 priority: school security."

Yet given the nature of gun violence at schools, Lockport's purchase of surveillance technology appears inefficient and expensive. All of the major school shootings in the last five years in the U.S. have been carried out by current students or alumnae of the school in question. "These are students for whom the school wouldn't have a reason to have their face entered into the face recognition system's blacklist," explained Rachel Levinson-Waldman, a security and policing expert at the Brennan Center for Justice.

Source

Human plus machine – face recognition at its best

A combination of human and computer decision-making is most accurate

The first study to compare performances of trained facial examiners, super-recognisers, and facial-recognition algorithms, has revealed a combination of human and computer decision-making is most accurate.

The first study to compare the performances of trained forensic facial examiners, people known as super-recognisers who have a natural talent for face identification, and facial-recognition computer algorithms, has revealed that a combination of human and computer decision-making is most accurate.

The study, by a team of scientists from the National Institute of Standards and Technology in the US and three universities including UNSW Sydney, is published in the Proceedings of the National Academy of Sciences.

"Experts in face identification often play a crucial role in criminal cases," says study team member, UNSW psychologist Dr David White.

"Deciding whether two images are of the same person, or two different people, can have profound consequences.

"When facial comparison evidence is presented in court, it can determine the outcome of a criminal trial. Errors on these decisions can potentially set a guilty person free, or wrongly convict an innocent person," he says.

The international study involved a total of 184 participants from five continents – a large number for an experiment of this type.

Eighty-seven were trained professional facial examiners, while 13 were super-recognisers – people with exceptional natural ability, but no training. The remaining 84 were control participants with no special training or natural ability, including 53 fingerprint examiners and 31 undergraduate students.

Source

Apple Granted Patents for iDevices with Ultrasonic Face & Backside Biometrics

Ultrasonic Fingerprint Sensors for iPhone
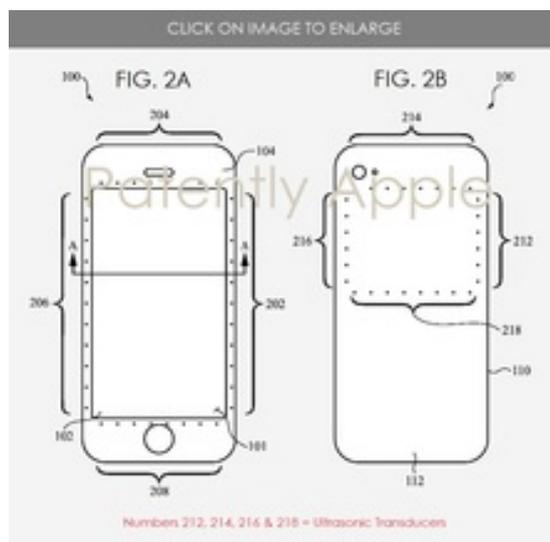
The U.S. Patent and Trademark Office officially published a series of 44 newly granted patents for Apple Inc. today. In this particular report we cover a fascinating new ultrasonic fingerprint sensor system that could be set on both the front and backside of an iDevice. This report also covers a fingerprint reader built into the display of an iDevice and built-in bezel controls for iDevices. Yet perhaps the most interesting granted patent of the day goes to a mysterious design patent for a possible future MacBook. A number of Apple's patent figures display a consistent mysterious element that will definitely leave you wondering what they might have up their sleeve.

Apple's newly granted patent covers their invention relating to an ultrasonic touch sensor that is configured to identify aspects of a touch on a device. The ultrasonic touch sensor may be configured to identify the location of a touch on a surface and/or identify biometric information associated with the touch.

In some embodiments, the biometric information includes a fingerprint associated with the touch. By identifying the fingerprint associated with a touch, the identity of the user can be verified, which may be useful for authorizing a transaction or performing a security operation.

Source

EAB Research Projects Conference 2018

The 5th edition of the EAB Research Projects Conference will take place on 24 and 25 September 2018, at the premises of Fraunhofer IGD in Darmstadt, Germany.

The conference is organized by the European Association on Biometrics (EAB) in cooperation with the Joint Research Center (DG JRC) of the European Commission, through its Cyber and Digital Citizens' security Unit. The EAB-RPC 2018 will be co-located with the EAB Research Award and the IEEE BIOSIG Conference, later that same week. The conference is currently the largest event on research funded by the European Union in the area of Biometrics and Identity Management.

Over the previous four successful editions, EAB-RPC has become the main forum in Europe where attendees can simultaneously: promote research carried out in biometrics, forge new links and networks, and identify the appropriate partners for possible future project applications. Last year's edition welcomed over 100 participants from academia, industry and public institutions.

SIS-II AFIS goes into operation

Created as a compensatory measure for the abolition of internal border checks within the Schengen area, the Schengen Information System (SIS) was established with two intentions: to contribute to law enforcement cooperation between the Member States and to support external border control.

The SIS was the first so-called large-scale IT system launched by the EU Member States in 1995. It was followed by EURODAC (asylum seekers' database) in 2003 and the Visa Information System (VIS) in 2011. The second generation of the system, SIS-II, entered into operation on the 9th of April of 2013 hosted by eu-LISA (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice). SIS-II enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects. Originally, consultations on person-related alerts could only be made on the basis of alphanumeric data (e.g., name, surname, date of birth). It was soon understood that such a searching procedure had limitations since criminals often change identities or use different aliases. In order to tackle such limitations SIS-II offers the possibility to store fingerprints linked to a person alert (as it is already the case for EURODAC and the VIS). However, initially, such biometric data could only be used to verify the identity of a subject already found through an alphanumeric search. According to Articles 22.c of the 2013 SIS-II Decision and Regulation , SIS-II could also be consulted to identify a person on the basis of his/her fingerprints. This option required the implementation of an Automatic Fingerprint Identification System (AFIS) "once it becomes technically possible" and when the Commission had presented "a report on the availability and readiness of the required technology on which the European Parliament is consulted". In October 2015 DG JRC provided such a report to DG HOME supporting the final decision of integrating 10-prints fingerprint identification technology within the functionalities of SIS-II . Based on the positive findings of the DG JRC study on the readiness of fingerprint recognition technology to be included in SIS-II, DG HOME consulted the European Parliament regarding this possibility. Following the approval by the Parliament, eu-LISA started the procedure for the integration of an AFIS in SIS-II. Finally, on the 5th of March 2018, the SIS-II AFIS went into the first phase of operation with the connection of 9 Member States that can now launch queries on the SIS-II database based on fingerprints. These 9 MSs will soon be followed by all European MSs and associated MSs.

To read more:

https://www.eulisa.europa.eu/Newsroom/News/Pages/eu-LISA-successfully-launches-SIS-II-AFIS-Phase-One.aspx