New hackproof Biometrics technologies for identification of criminal and national security suspects to law enforcement and military personnel.

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. A record of a person's unique characteristic is captured and kept in a database. Later on, when identification verification is required, a new record is captured and compared with the previous record in the database. If the software matches the data in the new record with that in the database record, the person's identity is confirmed, it then grants the appropriate level of access.

Fingerprint recognition is one of the oldest, simple to install, and low-cost technology; therefore, it finds numerous applications and is widely adopted by many industries. In travel and immigration, fingerprint recognition technology is used in e-passports, e-visas, and driving licenses to authenticate an individual. In the consumer electronics industry, fingerprint recognition technology is used in laptops, computers, and smartphones, among others.

Biometric verification has advanced considerably with the

advent of computerized databases and the digitization of analog data, allowing for almost instantaneous personal identification. The biometrics has now merged with other characteristics of physical body , for example Iris-pattern and retina-pattern authentication methods are already employed in some bank automatic teller machines. Apple announced plans for its “Face ID” feature, where you can unlock your iPhone X with your face. The applications have been developed that use a biometric marker, such as your fingerprint or your face, to access certain areas or pay for goods. Chinese coworking operator UrWork is partnering with the Alibaba fintech Ant Financial to create a fully staff-less experience in its flexible office workspaces using face recognition software and digital payment systems.

Military and Security require more technologically advanced methods of ensuring security against terrorist activities and Illegal immigration. One of the most effective methods of curbing the same is by creating biometric authentication across borders and airports.

Still, biometric data isn’t 100% secure. Just last year, 5.6 million federal employees’ fingerprint images were stolen. Databases get hacked all the time, from the IRS to Target to hospitals and banks, Universities are hacked every year, medical records, the IRS, banks, dating websites, the list goes on. “Biometric identification (perhaps at range) may strip away the anonymity that enables insurgents to blend into a society —or will allow future adversaries to identify, track, isolate, and target individual U.S. political or military leaders,” writes DOD report.

Bio-metric technologies

Voice waveform recognition, a method of verification that has been used for many years with tape recordings in telephone wiretaps, is now being used for access to proprietary databanks in research facilities.

Facial-recognition technology has been used by law enforcement to pick out individuals in large crowds with considerable reliability. Facial recognition is going to play an increasing role, especially in surveillance and border security applications, due to increasing concerns about terrorism and mass migration

Hand geometry is being used in industry to provide physical access to buildings. Earlobe geometry has been used to disprove the identity of individuals who claim to be someone they are not (identity theft). “Ears are unique,” says Michael Boczek, the President and CEO of Descartes Biometrics, a company that specializes in mobile ear detection security apps. “It’s stable and enduring, which means it changes very little over the course of one’s life. That’s also true of fingerprints, but less true of facial recognition.”

The concept of a ‘Vein ID’ technology brings further benefits, finger-vein remains the same throughout the life, and is completely unique to you. “Payment by vein” technology is already being trialled at a supermarket in Brunel University London, UK. An electronic reader maps the user’s finger veins, generating a unique key. The beauty with your vein is that it sits below your skin, and can only be seen when shining infrared light through your finger, making it much more difficult to see and replicate. “While all

biometrics have their strength and weaknesses, finger-vein is the most secure," claims director, Simon Binns of Sthaler, the company behind the Fingopay technology.

Signature comparison is not as reliable, all by itself, as the other biometric verification methods but offers an extra layer of verification when used in conjunction with one or more other methods.

Mobile Bio metrics

Apple has included TouchID in every iPhone from the 5S onwards, and Microsoft has included a face scanning unlock feature with Windows 10. Google offers glass wearable technology with an optical head-mounted display that enables individuals to access their credentials with voice and facial recognition and has the capability to perform individual identification and verify customers. The law enforcement agencies in Dubai are planning to use Google Glass with a facial recognition software for field operation to capture photos of individuals and search their faces in the criminal database to identify any potential suspects.

Biometrics are being introduced in many wearable devices like smart watches, ear-pods, bands, and eyeglasses. These devices have biometric identification capabilities and can identify an individual's biometric traits like heart rate and blood pressure.

MasterCard has partnered with the biometrics company Nymi to test heartbeat authentication for credit card purchases. Wearable biometric identification devices with different biometric authentication capabilities are available

in the market for various purposes. EyeVerify, works by scanning the blood vessel patterns in the whites of your eye by using a selfie taken with a smartphone. Other mobile phone companies have built devices that use infrared cameras to scan irises.

Researchers improving facial recognition performance

Chinese police have used facial recognition technology to catch criminals at a beer festival. Those caught included one man who had been on the run for 10 years. Eighteen cameras installed at four entrances to the festival identified each of the suspects in under one second, Qingdao police said.

Dozens of other people with criminal records or a history of drug abuse were refused entrance after computers spotted them. According to Qingdao authorities, the system has a 98.1% accuracy rate and sounds an alarm if a subject's face is found in the police database. Six officers were stationed at each entrance to verify the matches.

China is racing ahead in its use of facial recognition technology, despite widespread concerns about its impact on privacy and civil liberties. It has been installed at Beijing's historic Temple of Heaven to stop people stealing rolls of toilet paper, and this year China Southern Airlines used facial recognition in place of boarding passes for the first time.

A team of researchers from Maryland's U.S. Army Research

Laboratory have developed a new technique exploiting thermal-imaging that potentially could help improve facial-recognition performance that is otherwise hindered by makeup. Developed by Doctors Nathaniel Short, Alex Yuffa, Gorden Videen, and Shuowen Hu, the new method compares visible, conventional thermal and polarimetric-thermal images of faces before and after the application of face paint.

The researchers have been using polarimetric-thermal imaging, a maturing thermal mode that records the polarization-state information of thermal infrared emission, to collect geometric facial data from thermal imagery. This method could provide several advantages over conventional thermal imaging when matching faces with paints or cosmetics, said Short.The research team describe their findings in The Optical Society (OSA) journal, Applied Optics.

Traditional facial-recognition systems are based on matching clear and well-lit photos captured in the broad light. Recognizing faces using visible-light imaging depends on capturing the reflected light from the edges of facial features. This can be difficult when faces are covered with cosmetics as they tend to distort the perceived shape of the face and degrade the face-recognition accuracy of visual imaging due to the different spectral properties of color pigmentation. In comparison, infrared, thermal signature is naturally emitted from the human face and can be attained passively in low-illumination conditions and even if face paints or cosmetics cover the skin’s surface.

Despite this promising research, Short emphasizes that the development of the new facial-recognition technique is still in its initial stages and that many challenges still

exist. “One of the major challenges is the limitation of the existing polarimetric-thermal facial database,” said Short. “Large sample pools are needed to develop and train complex machine-learning techniques such as neural networks computer programs that attempt to imitate the human brain to make connections and draw conclusions.” Another key challenge is in developing algorithms that bridge the large modality gap between visible imaging and polarimetric-thermal imaging for cross-spectrum recognition.

Behavior ID

Mobile identification company TeleSign launched Behavior ID , an online application that tracks a user’s behavior to prevent cybertheft. The application records behavior such as how a user moves their mouse, presses a touch screen, or the way they type. This increases the level of identity assurance for every user account a company has, according to Steve Jillings, CEO of TeleSign.

“The power of Behavior ID is its ability to adapt to the user, transparently producing a digital fingerprint from a user’s behavior to confirm their identity and develop an ongoing authentication without requiring the consumer to do anything,” he said in a press release. “Best of all, these unique biometric patterns are extremely accurate, from the way we move our hand on a mobile device screen or with a mouse, it is virtually impossible to precisely imitate another person’s behavior.”

Eventually, we could even see biometrics able to identify people by their brain waves. Since as early as 2013, researchers have been studying a way to record brain signals

using an electroencephalogram, a monitoring test historically used to diagnose epilepsy, tumors and other disorders.

Military and Security Requirements

“In the initial aftermath of 9/11, government officials immediately recognized the need for improved border control and automated systems for identifying individuals trying to enter the country. New biometrics technologies offered one means of verifying identities and comparing these records against watchlists of potential threats gathered by DoD and other government agencies,” writes COL Glenn Voelz, USA.

“As the United States shifted towards a counterinsurgency strategy, it required population-centric information and refined targeting intelligence for identifying, isolating, and eliminating insurgents from the battlefield. These operational challenges demanded new technologies to enable U.S. forces to detect and identify individual actors, characterize and geo-locate their activities, and understand the structure and function of their networks. This presented an enormous tactical dilemma for soldiers fighting on an irregular battlefield against adversaries who did not wear uniforms and could not easily be distinguished from the local population. As such, identity verification emerged as one of the major technical challenges of the campaigns in Iraq and Afghanistan,”writes COL Glenn Voelz, USA.

In early 2002, a BAT prototype was fielded to Joint Special Operations Command in Afghanistan and first used for enrolling persons of interest detained on the battlefield. By 2003, similar systems were deployed at detention facilities in Iraq for detainee management and later as a tool for generating

biometrically enhanced interrogation reporting (Iasso, 2013). By 2004, DoD directed that all U.S. military units worldwide would collect biometric data from detainees (DoD, 2004). One vivid demonstration of the value of this data came in 2011 when 500 Taliban prisoners escaped from Kandahar's Sarposa prison. All detainees had previously undergone biometric enrollment, and within 1 month 30 individuals were recaptured in the local area as a result of random biometric checks.

In this complex human terrain, biometric technologies helped put a uniform on the nation's enemies and reduced their ability to leverage anonymity for military advantage. Technavio defense research analyst Moutushi Saha asserts in a report summary that the "US military has been using iris scan technology for over a decade in Iraq and Afghanistan to authorize selected individual's entry into the military facilities in the US bases." Such access control applications will continue to be important, but iris scanning is also finding its way into other areas such as passport control and civil ID, as seen in India's Aadhaar program.

The U.S. Army Special Operations Command (SOCOM) (www.soc.mil) has posted a request for information (RFT) to evaluate selected exploitation technologies. It seeks technologies including collection, segregation and matching of voice from media or live capture. Rapid DNA hand-held collection, processing, and matching technologies; facial recognition up to one kilometer and dustless fingerprint collection.

According to the report, several government agencies are using biometric technologies for local, state, and federal criminal investigations. In January 2016, the FBI of the US opened a

Biometrics Technology Center in North Central West Virginia. The new facility has advanced biometric identification and recognition technology, using human characteristics that provide identification of criminal and national security suspects to law enforcement and military personnel. In March 2016, Northrop Grumman received a contract from the US Army to supply biometric technology to manage investigations, threat inquiries, and other activities associated with the complaints registered and inquiries about any illegal leaks of confidential national security information.

Iris ID Tech Adopted for Military Communications

The company has announced that its iris recognition technology has been incorporated into Ultra Electronics' military-focused product portfolio, with integrations into the latest Combat Apps Tactical System (CATS) tablets.

The tablets are designed to offer encrypted, high-speed communications between troops in the field and administrators at headquarters, and will now use Iris ID's R-100 camera and IrisAccelerator matching software to authenticate soldiers' identities, matching their iris biometrics against databases stored at military bases.

Iris ID business development and sales VP Mohammed Murad suggested that the technology's track record points to military applications, asserting that "Iris ID technology has been proven effective worldwide in remote locations and during extreme weather conditions for national ID and other programs.

Security of Biometrics

“Biometrics are tricky,” Woodrow Hartzog, an Associate Professor of Law at Samford University told WIRED. “They can be great because they are really secure. It’s hard to fake someone’s ear, eye, gait, or other things that make an individual uniquely identifiable. But if a biometric is compromised, you’re done. You can’t get another ear.”

Biometric data isn’t immune to these attacks. For instance, at the CCC conference in 2014, a security researcher called Starbug used a simple 3D printed mold to construct a working model of the German Defence Miniser’s fingerprint which was based on a high-res photograph of the minister’s hand. And researchers at Michigan State University released a paper that describes a method for spoofing a fingerprint reader using conductive ink printed with an ink jet printer in less than fifteen minutes.

Voice recognition application ‘Siri’ has also faced several security issues. In 2011, a China-based hacker group managed to jailbreak the iPhone 4 and run a full version of Siri which allowed them to steal sensitive information from the users who installed the app. At the same time, according to various security researchers, a sample of user’s voice can be collected in various ways including making a spam call, recording person’s voice from a physical proximity of the speaker, mining for audiovisual clips online and compromising cloud servers that store audio information.

In fact researchers from mobile security firm Vkansee were able to break into Apple’s Touch ID system with a small piece of Play Doh just last month at the Mobile World

Congress—similar to what security researcher Tsutomu Matsumoto a did with a gummy bear over a decade earlier with another fingerprint sensor. Many commercially available iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face.

Although many experts say biometrics are intrinsically secure (since no one else can have your ears or eyes), Alvaro Bedoya, Professor of Law at Georgetown University, argues otherwise. “A password is inherently private. The whole point of a password is that you don’t tell anyone about it. A credit card is inherently private in the sense that you only have one credit card.”

“As far as passwords go, they are widely recognized by security experts as a very poor authentication mechanism, mostly due to people’s inability to choose long, unguessable passwords,” he told CNBC via email.

Biometrics, on the other hand, are inherently public, he argues. “I do know what your ear looks like, if I meet you, and I can take a high resolution photo of it from afar,” says Bedoya. “I know what your fingerprint looks like if we have a drink and you leave your fingerprints on the pint glass.” And that makes them easy to hack. Or track.

Biometric solutions are still not perfect and the technology can make mistakes. Recognition software has yet to mature, so it can misread an image and block access to the authorized user. “Facial recognition is a good example of biometric authentication that can still prove challenging to implement

as it tends to be prone to a high false positive rate” Siân John, EMEA chief strategist at Symantec, told CNBC via email. Other variables also reveal mobile biometrics’ weak spots. Scanner hardware can malfunction if it gets smudged or scratched.

Market growth

According to TMR, the global military biometrics market is expected to report a CAGR of 7.4% between 2017 and 2025. At this pace, the market’s valuation will reach US$10.62 bn by the end of 2025, from US$5.65 in 2016. The future growth of the biometric system market is expected to be driven by rising use of biometric technology in financial institutes and healthcare sectors, government initiative in adoption of biometrics system, and increasing use of biometric systems in criminal identification.

The global military biometrics market is highly competitive, as its vendor landscape is marked by the presence of several large global players. The dominance in the market is however held by five major players – 3M Cogent, NEC Corporation, M2SYS Technology, Crossmatch, and Safran. Together these companies accounted for nearly 61% of the global military biometric market in 2016. Other Major players in this market include Fujitsu Ltd. (Japan), BIO-Key International, Inc. (U.S.), Precise Biometrics AB (Sweden), Secunet Security Networks AG (Germany), Thales SA (France), Aware, Inc. (U.S.), Cognitec Systems GmbH (Germany), Fulcrum Biometrics, LLC (U.S.), Daon, Inc. (U.S.), and Facebanx (U.K.).

Despite recent innovations, integration complexities still prevalent in military biometric technologies are hindering the

market’s trajectory. It is very important to correctly configure any biometric system and feed it with proper data for it to function correctly. Any loophole in the integration process can cost organizations big time. Also if the system gets compromised with at any point, it could result in security breach, for it is highly time- and labor-consuming to reset the whole system. Such integration complexities pose big risk to the defense sector as it involves highly confidential data related to their country. This could be a major deterrent for the military biometrics market.

References and Resources also include:

http://www.prnewswire.com/news-releases/global-military-biometrics-market-growth-at-75-2016-2020—technologies-being-used-for-local-state—federal-investigations—research-and-markets-300378942.html

http://searchsecurity.techtarget.com/definition/biometric-verificationhttps://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/http://www.allaboutcircuits.com/news/biometric-security-measures-can-be-hacked-easily/http://www.deccanchronicle.com/technology/in-other-news/111016/biometrics-technology-the-past-present-and-future.html

http://www.cnbc.com/2016/04/05/biometrics-future-of-digital-cyber-security.html

http://www.marketsandmarkets.com/PressReleases/biometric-technologies.asp

http://findbiometrics.com/military-iris-facial-biometrics-312156/#

http://www.dau.mil/publications/DefenseARJ/ARJ/ARJ77/ARJ77-Voe

lz_Article03.pdf

http://www.biometricupdate.com/201606/researchers-develop-new-technique-that-could-improve-facial-recognition-performance

http://finance.yahoo.com/news/military-biometrics-market-demand-advanced-103000804.html

https://www.theguardian.com/world/2017/sep/01/facial-recognition-china-beer-festival