Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
A research team from the University of Southern California (USC) have developed new algorithms that can detect biometric attacks on iris, facial and fingerprint recognition systems with high levels of accuracy.

The researchers, from USC’s Information Sciences Institute, have announced the early results from their study, titled ‘Biometric Authentication with Timeless Learner’ (BATL).

The driver for BATL was the increase in spoof attacks as biometric authentication becomes widespread. To combat this, the researchers developed systems and algorithms designed to stop criminals spoofing photos or fingerprints to break into personal devices. These systems were then subjected to three weeks of testing at the independent John Hopkins Applied Physics Laboratory (APL), where a range of spoofing attacks were used to try to break them.

Using data collected from about 700 participants, APL found that the facial biometric system had a 100% accuracy rate, as it didn’t make a single mistake in identifying attacks. The iris recognition system had an overall accuracy of 99.36% and the fingerprint recognition systems 99.08%, both figures higher than the researchers expected.

BATL is being funded under the Intelligence Advanced Research Projects Activity (IARPA) Odin programme to strengthen biometric security systems.

Project leader Wael AbdAlmageed, research associate professor at USC Viterbi’s Department of Electrical and Computer Engineering, said: “BATL’s goal is to create novel sensing hardware for face, fingerprint and iris biometrics that provide unconventional data sources. Our aim is to develop state-of-the-art machine learning and artificial intelligence algorithms that can quickly and accurately detect biometric attacks.”

The fingerprint system developed by the BATL team was contactless, which they believe is significant for organisations using legacy fingerprint systems in the Covid-19 era.

ISI machine learning and computer vision scientist, Hengameh Mirzaalian, who worked on this element of the project, explained: “The nice thing about our fingerprint station is that it’s touchless, making it less vulnerable to fingerprint lifting and is more desirable from the hygiene perspective. This is a super valuable feature in this Covid-19 era.”

More information on BATL is provided in a post on the USC Viterbi blog.

**FINGERPRINTING**

**Could slime be the answer to fingerprint crime?**

A research project at the University of Toronto has tested whether a popular type of household ‘slime’ favoured by children can be used to enhance fingerprints and help solve crimes.

Toronto Mississauga forensic science graduate Leanne Byrne set out to test a technique originally devised by American forensic investigator Caleb Foster – that applying a popular children’s ‘slime’ to hard-to-see fingerprints would make them visible enough to be used in forensic investigations.

She carried out an independent study, co-authored by University of Toronto forensic identification instructor Wade Knapp and lab technician Agata Gapinkska-Serwin. Byrne revised Foster’s method of mixing a chemical reagent with a rubbery slime compound.

She focused on testing two reagent compounds often used by investigators: crystal violet and amido black.

“My method proposes an inexpensive technique that uses borax mixed with glue as the baseline compound. Reagent agents in the slime react with the fingerprint, producing a stain that enhances the detail so we can graph it,” she said.

Byrne tested bloody and non-bloody prints of different ages. She also tested the slime mixtures on different surfaces, including black electrical tape, beige and clear packing tapes, silver duct tape and painted wood tiles. The results were encouraging. “The best enhancement was produced on black electrical tape and beige packing tapes,” Byrne said. “It didn’t work as well with clear and duct tapes, so the technique is better for some surfaces than others.”

She found the technique enhanced hard-to-see details, as seen in the pictured example of a bloody fingerprint before and after application of the amido black slime compound.

Byrne believes the results justify further testing using other chemical reagents with different surfaces and variable fingerprint conditions. “Fingerprints can change over time, depending on the environment and variables like temperature and humidity,” she said. “We want to make sure that a technique is going to work consistently regardless of the age.”

Byrne has graduated after gaining a high distinction in Toronto’s honours bachelor of science programme. She plans to pursue a career as a forensic

---

**CYBER-SECURITY**

**USC team develop accurate anti-spoofing**

A research team from the University of Southern California (USC) have developed new algorithms that will authenticate their identity against the ID document. This will include ‘genuine presence’ checks to confirm the user is a real person, rather than a photo, video or mask. “This protects against large-scale criminal attacks using deepfakes,” iProov said. Once their identity is established, passengers will not need to show their ticket or passport until they reached their destination.

The iProov solution is being developed in partnership with Eurostar and Canadian travel and immigration solution specialist WorldReach Software.

Eurostar strategy director Gareth Williams said: “We are very pleased to be working with iProov on this important innovation. We’re convinced it will enhance our passenger experience and offer a live illustration of how our innovation can benefit the high-speed rail and international transport industries.”

“With high levels of accuracy, and fingerprint recognition systems designed to stop criminals spoofing photos or fingerprints to break into personal devices, these systems were then subjected to three weeks of testing at the independent John Hopkins Applied Physics Laboratory (APL), where a range of spoofing attacks were used to try to break them.”