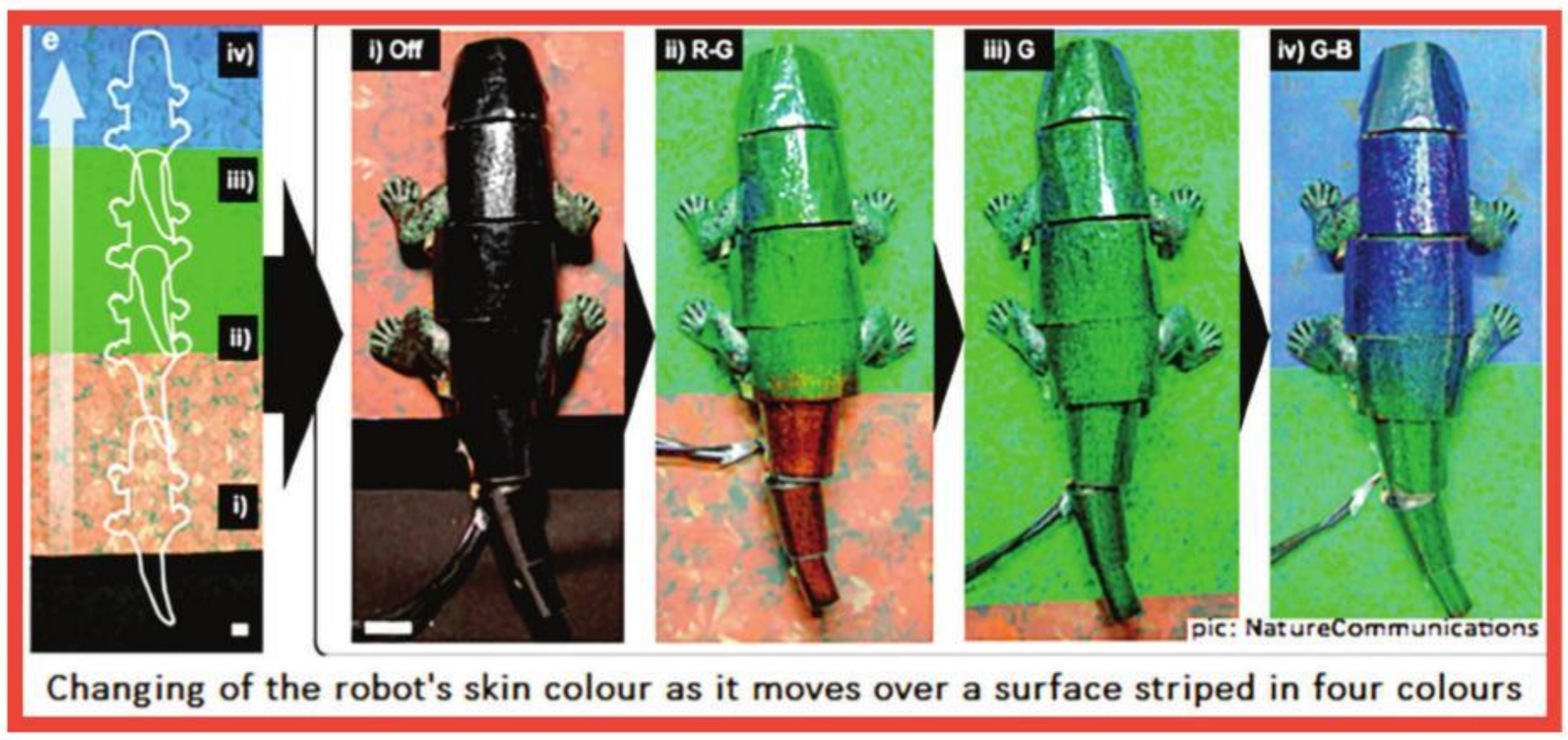

Changing of the robot's skin colour as it moves over a surface striped in four colours

Doing it like the chameleon

A research team from South Korea has created a robotic model that mimics nature's leader of camouflage

S ANANTHANARAYANAN

Camouflage is a strategy of nature. Armies use it in defence and attack, and there are many fields where merging physically with the environment is an advantage.

In the natural world, however, to stay unseen is an imperative. The hunted need to stay out of sight, and predators cannot be successful if their presence is discovered by their prey. A classic instance of staying hidden is that of the butterfly, *Kallima inachus*, which is black, orange and blue, when the wings are open, but resembles a dead leaf when the wings are closed. As for predators, few can match the crocodile, which floats at the edge of a pond, like a log, till an animal comes there to drink!

Hyeonseok Kim, Joonhwa Choi, Kyun Kyu Kim, Phillip Won, Sukjoon Hong and Seung Hwan Ko, from Seoul National University and Hanyang University in South Korea, describe in the journal, *Nature Communications*, an artificial surface that mimics nature's leader in adapting its appearance to surroundings — the chameleon's capacity to rapidly change colours.

The colours in nature arise either due to pigments or the structure of surfaces. The colours of flowers and leaves, and even of animal skin, are because of the chemicals that they contain. Most of the colour-related action is in cells that contain pigment, which can be red, dark, as in black, or yellow. And there are animals, particularly marine animals, that can control the pigments expressed, and are able to bring about an extent of changes in colours. Many marine species also have fluorescent or bioluminescent scales. The squid is even known to harbour bacteria that glow to match a well-lit background and avoid being seen by predators.

The feathers of many birds, fish scales, or insect surfaces, however, rely more on physical structure, which causes some of the wavelengths found in natural light to be reflected strongly. The effect is similar to the rainbow colours that we can see on a film of oil spilt on a puddle, and the colours can change with the angle of view as the animal moves.

The changes in colours of the chameleon was considered to arise from dispersion, or the coming together, of light-reflecting cells which contain pigments. But some species of chameleon show great variations of colour, not just of shade. As this cannot arise by only changing the distribution of pigment-carrying cells, scientists have looked deeper. It has been found that the skin of the male chameleon contains two layers of a mesh of minute crystals, which have no affinity to colours, but whose orientation and separation affects the shades of light that the skin reflects.

The chameleon's ability to rapidly change colours is through muscular changes in the distances between the nanocrystals, which change the wavelengths of light that are strongly reflected by the animal's skin.

Artificial camouflage

Developing an artificial camouflage system that compares with the standard that the chameleon has set presents a huge challenge, the *Nature Communications* paper says. The paper recalls that ever since the 1800s, there have been efforts to develop technology that could help the military, either to evade detection or see through camouflage used by the enemy. And surface covers that would match the background, either in colour or a pattern, have been the objectives. The challenge is — even just for matching the background colour, the device used would need to cover the visible spectrum, and switch colours with the least delay.

One way to meet the requirements would be to build each pixel to contain a panel of devices, one for each colour. For reasonable resolution, however, the devices would need to be densely packed. And the device itself needs to be flexible and mechanically robust. All this, and the need to sense the colour of the background, and communicate with individual units, leads to an explosive increase in the system complexity, the paper says.

The solution that the team in South Korea has found is to build the surface with an ink that changes colour according to temperature — consisting of what are termed as "thermochromatic liquid crystals". The TLC is a device that changes colour, depending on the temperature. So far, the TLC is mainly used as a "non-invasive temperature indicator", for example of moving liquids. But the material has a range that covers the visible spectrum, and, the paper says, the TLC has been acknowledged as a potential candidate for artificial camouflage applications.

In the work of the South Korean group, the TLC layer is backed by a stack of transparent sheets that carry silver nanowire heaters. With patterning of the nanowires, it is possible to control temperature at individual spots of the TLC layer, to display the desired colours. Once a proper control circuit is provided, the paper says, it becomes possible to have sensitive temperature management, and without the need for packing individual units for pixels of each colour.

"The silver nanowire has excellent electrical conductivity and oxidation resistance as a single material and has a cost-effective feature to be applied for large-area applications through a simple synthesis process," the paper says. The electrical resistance varies according to temperature, and it becomes a way to know the temperature of a nanowire heater, so that the temperature can be controlled, which "permits a further reduction in the response time, even to be comparable to the physiological colour change found in animals," the paper says.

Using such ideas, the South Korean team has created a "robotic chameleon" — a model that is equipped with the silver nanowire and TLC-based "artificial chameleon skin", and then with colour sensors and feedback control systems. The result is an "adaptive artificial camouflage…device which is capable of detecting the local background colour and matching its colouration in real-time,", the paper says.

The team recognises that in most habitats, it is only the background colour that needs to be matched, not a complicated image. With that in mind, in place of constructing a large number of heater elements, the layers were built with void areas and patterned according to common habitats. Stacking of such layers allowed simultaneous colour matching and expression of the microhabitat, and with greatly reduced complexity of construction.

The technology developed could have applications in diverse areas like architecture, art, fashion, and consumer products, apart from military applications.

The writer can be contacted at response@simplescience.in

PLUS POINTS

Robot swarms' decisions

New research that could help us use swarms of robots to tackle forest fires, conduct search and rescue operations at sea and diagnose problems inside the human body, has been published by engineers in the United Kingdom. The study could improve how swarms of robots work together, adapt to changes in their environment and make more sophisticated decisions much quicker.

Published in the journal *Science Robotics*, the paper called "When Less is More: Robot swarms adapt better to changes with constrained communication", has found that robot swarms are able to respond more effectively to changes in their environment when communication between robots is reduced. The study disproves the widely accepted theory that more connections between robots lead to more effective information exchange.

The team, which included researchers from University College London, University of Sheffield, and the Institute for Interdisciplinary Studies on Artificial Intelligence, Université Libre de Bruxelles, Belgium, discovered their findings by studying how a swarm of tiny robots moved around and reached a consensus on the best area (for example, most urgent or best suited to perform a task) they should gather in and explore.

Each robot assessed the environment individually, made its own decision on the best area and broadcast its opinion to the rest of the swarm. Every robot in the swarm then periodically selected a random assessment that had been broadcast by another robot in the swarm and used it to update its opinion on the best area — a protocol known in robotics as the "voter model". Once every robot had gone through this process the swarm reached a consensus on the best area to gather and explore based on the opinion of each robot.

The team, however, found that by using this protocol the robot swarm was slow to adapt to changes in the environment when a better site appeared. The researchers then discovered that when robots only communicated to other robots that were within a 10-centimetre range — rather than broadcasting their message to the whole group — the swarm was able to adapt to changes in their environment much quicker and select the best available area.

Andreagiovanni Reina (*in photo*), who led the study, is a research fellow of the Belgian National Fund for Scientific Research at the Institute for Interdisciplinary Studies on Artificial Intelligence of the Université Libre de Bruxelles and University of Sheffield's department of computer science. He said, "Swarms of robots have huge potential to help us access places that are either too hazardous or simply inaccessible to humans. For example, they could fly over a forest fire that is too vast or dangerous for humans to tackle alone, monitor how the fire spreads and decide where help is needed the most.

"What happens, however, if the fire suddenly changes direction and support is urgently needed elsewhere — the swarm of robots needs to be able to quickly adapt to this change and identify where urgent support is needed.

"This is what our research is helping to do — our findings could be used to develop swarms of robots that are more responsive and able to make the right decisions much quicker than they currently can do."

WHAT IS PEGASUS?

A cybersecurity expert explains how the spyware invades phones and what it does when it gets in

BHANUKIRAN GURIJALA

End-to-end encryption is technology that scrambles messages on your phone and unscrambles them only on the recipients' phones, which means anyone who intercepts the messages in between can't read them. Dropbox, Facebook, Google, Microsoft, Twitter and Yahoo are among the companies whose apps and services use end-to-end encryption.

This kind of encryption is good for protecting your privacy, but governments don't like it because it makes it difficult for them to spy on people, whether tracking criminals and terrorists or, as some governments have been known to do, snooping on dissidents, protesters and journalists. Enter an Israeli technology firm called the NSO Group, named after founders Niv Carmi, Shalev Hulio and Omri Lavie.

The company's flagship product is Pegasus, spyware that can stealthily enter a smartphone and gain access to everything on it, including its camera and microphone. Pegasus is designed to infiltrate devices running Android, Blackberry, iOS and Symbian operating systems and turn them into surveillance devices. The company says it sells Pegasus only to governments and only for the purposes of tracking criminals and terrorists.

How it works

Earlier versions of Pegasus were installed on smartphones through vulnerabilities in commonly used apps or by spear-phishing, which involves tricking a targeted user into clicking a link or opening a document that secretly installs the software. It can also be installed over a wireless transceiver located near a target, or manually if an agent can steal the target's phone.

Since 2019, Pegasus users have been able to install the software on smartphones with a missed call on *WhatsApp*, and can even delete the record of the missed call, making it impossible for the phone's owner to know anything is amiss. Another way is by simply sending a message to a user's phone that produces no notification.

This means the latest version of this spyware does not require the smartphone user to do anything. All that is required for a successful spyware attack and installation is having a particular vulnerable app or operating system installed on the device. This is known as a zero-click exploit.

Once installed, Pegasus can theoretically harvest any data from the device and transmit it back to the attacker. It can steal photos and videos, recordings, location records, communications, web searches, passwords, call logs and social media posts. It also has the capability to activate cameras and microphones for real-time surveillance without the permission or knowledge of the user.

Who has been using Pegasus and why

NSO Group says it builds Pegasus solely for governments to use in counterterrorism and law enforcement work. The company markets it as a targeted spying tool to track criminals and terrorists and not for mass surveillance. The company does not disclose its clients.

The earliest reported use of Pegasus was by the Mexican government in 2011 to track notorious drug baron Joaquín "El Chapo" Guzmán. The tool was also reportedly used to track people close to murdered Saudi journalist Jamal Khashoggi.

It is unclear who or what types of people are being targeted and why. However, much of the recent reporting about Pegasus centres on a list of 50,000 phone numbers. The list has been attributed to NSO Group, but the list's origins are unclear. A statement from Amnesty International in Israel stated that the list contains phone numbers that were marked as "of interest" to NSO's various clients, though it's not known if any of the phones associated with numbers have actually been tracked.

A media consortium, the Pegasus Project, analysed the phone numbers on the list and identified more than 1,000 people in over 50 countries. The findings included people who appear to fall outside of the NSO Group's restriction to investigations of criminal and terrorist activity. These include politicians, government workers, journalists, human rights activists, business executives and Arab royal family members.

Other ways your phone can be tracked

Pegasus is breath-taking in its stealth and its seeming ability to take complete control of someone's phone, but it's not the only way people can be spied on through their phones. Some of the ways phones can aid surveillance and undermine privacy include location tracking, eavesdropping, malware and collecting data from sensors.

Governments and phone companies can track a phone's location by tracking cell signals from cell tower transceivers and cell transceiver simulators like the StingRay device. Wi-Fi and Bluetooth signals can also be used to track phones. In some cases, apps and web browsers can determine a phone's location.

Eavesdropping on communications is harder to accomplish than tracking, but it is possible in situations in which encryption is weak or lacking. Some types of malware can compromise privacy by accessing data.

The National Security Agency of the United States has sought agreements with technology companies under which they would give the agency special access into their products via backdoors and has reportedly built backdoors on its own. The companies say that backdoors defeat the purpose of end-to-end encryption.

The good news is, depending on who you are, you're unlikely to be targeted by a government wielding Pegasus. The bad news is, that fact alone does not guarantee your privacy.

The writer is assistant professor of computer science and information systems, West Virginia University, United States. This article first appeared on www.theconversation.com