I) Image recognition app scans paintings to act like Shazam for art

This will look nice in the digital gallery

Ross Harrison

By Matt Reynolds

Taking a souvenir home from an art gallery no longer has to mean a trip to the gift shop. A new app lets people scan a work of art with their smartphone camera to find out more about it and save a digital copy.

The app, called Smartify, uses image recognition to identify scanned artworks and provide people with additional information about them. Users can then add the works to their own digital collection. Smartify co-founder Thanos Kokkiniotis describes it as a combination of the music discovery service Spotify and music recognition app Shazam – but for visual works.

The app will launch in May for selected artworks at the Louvre in Paris, France, and the Metropolitan Museum of Art in New York, and all the artworks at the Rijksmuseum in Amsterdam and the Wallace Collection in London.

Many museums and galleries have apps to tell visitors more about their collections, but Smartify will work across institutions. You also won't need to visit an original work to get the benefit: scan a postcard of Leonardo da Vinci's *Mona Lisa* and the app will bring up information in the same way as if you were standing in front of it at the Louvre.

Creating an app that can recognise individual paintings is relatively easy because most galleries already have digitised versions of their collections, says Kokkiniotis. The challenging part is convincing galleries to let the app access this information. Then it's a matter of matching up what's seen through the smartphone camera with the database of digitised artworks.

Digital complement

Other digital collections, such as Google's Art Project, showcase digital versions of paintings and offer virtual tours around galleries, but Smartify is intended to complement real-world visits to galleries and not just act as an online image database.

Kokkiniotis hopes that more institutions and individual artists will make their works available as the app grows in popularity. Museums and galleries that sign up will also be able to access demographic information about people who use Smartify and the artworks they interact with, which they could use to inform their marketing and advertising. People logging into the app will have their data anonymised, says co-founder Anna Lowe. If they don't want to share their data, they can use the app without logging in.

But not everyone is so enthusiastic about people using smartphones in galleries. "Many visitors go to museums to have an unplugged experience," says Kevin Walker at the Royal College of Art in London.

He thinks visitors should look up from their phones and put their trust in gallery curators when it comes to viewing works of art. "They're the experts in experience," he says.

II) Chinese tourist town uses face recognition as an entry pass

We have a match!

Baidu

By Timothy Revell

Who needs tickets when you have a face? From today, the ticketed tourist town of Wuzhen in China is using face-recognition technology to identify people staying in its hotels and to act as their entry pass through the gates of the attraction.

The system, which is expected to process 5000 visitors a day, has been created by web giant Baidu – often referred to as the "Chinese Google".

Wuzhen is a historic town that has been turned into a tourist attraction with museums, tours and traditional crafts. When people check in to hotels in the tourist area, they will now have their pictures taken and uploaded to a central database. If they leave and

re-enter the town, the face-recognition software will check that they are actually a guest of a hotel there before allowing them back in.

Previously, multiple types of entry ticket had to be handed out to distinguish between one-off visitors and those staying for longer. But the system could easily be exploited, and some guests were caught sharing their tickets with other people to avoid paying the entry fee.

To prevent this, the town started to use fingerprint identification for hotel guests, so only one individual could use each entry pass. "But this took too long," says Yuanqing Lin, director of the Institute of Deep Learning at Baidu.

Asking visitors to put their finger on a sensor and wait for software to verify their identity caused big queues and often resulted in false positives. The new face-recognition system uses cameras to spot people as they approach a turnstile at the entry. Faces detected by the cameras are checked against a database of registered visitors, all within a second. If you're on the database, you're allowed in; if not, the doors remain closed.

Facing the cameras

"It was only a matter of time before face-recognition software was rolled out on this scale," says Mark Nixon at the University of Southampton, UK. It's more convenient to use your face than tickets, he says, so it's likely that the technology will soon be seen elsewhere.

Baidu's face-recognition software uses neural networks – a technique inspired by neurons in the brain that helps to recognise complex patterns. The company has trained the software on huge data sets that together total more than 1 billion images of people's faces and says that the system has an accuracy of 99.8 per cent, although this was achieved by examining still images rather than people walking up to a camera.

The software also detects facial movements, so can't be fooled by someone holding up a still image of another person's face.

The system is first being used to track the 5000 people per day staying in hotels in Wuzhen, who make up around 15 to 20 per cent of the town's total visitors. Baidu is already using the software for employee entry at its Beijing headquarters, but this is the first time it will be rolled out at such a scale.

Privacy concerns

Some airports already have a form of face-recognition software at passport control, but the setup is different. At an airport, you have to present your passport and the software determines whether the person standing in front of the camera matches that identity. But at the gates of Wuzhen, no identification is presented: instead, the software searches a large database for the face staring into the camera.

Compiling a database of faces in this way presents privacy concerns. Lin says the responsibility for storing the data falls to the Wuzhen attraction that uses it, not Baidu.

"In China, there is not a single overarching privacy law, but companies do have obligations to keep data safe," says Tiffany Li, an affiliate of the Center for Information Technology Policy at Princeton University.

Companies around the world are building large databases of personal information, with some starting to store biometric information such as fingerprints too. "This will make it easier to log on to your bank, but it will also be more of an issue if the database is hacked," says Li.

If the Wuzhen trial is successful, Baidu hopes to operate similar systems elsewhere, such as at other tourist spots and theme parks. "We want our software to eventually be used by all of the town's visitors, and then in many other places around China," says Lin.

III) Police mass face recognition in the US will net innocent people

Face it, you're nicked

John Moore/Getty

By Hal Hodson

Live in the US? There's a 50:50 chance that you're in a police face recognition database, according to a report from the Center on Privacy & Technology at Georgetown Law in Washington DC. The findings suggest that about a quarter of all police departments in the US have access to face recognition technology.

That police are using face recognition technology is not a problem in itself. In a world with a camera in every pocket, they would be daft not to. But face recognition can be used far more broadly than fingerprint recognition, which means it carries a higher risk of tagging innocent people.

Fingerprints are difficult to work with. Prints from known criminals can only be gathered in controlled environments at police stations, and dusting for prints is so time consuming that it is only done at relevant crime scenes. This narrows down the number of people in the sights of any one investigation.

.

It's much easier to build huge databases of identified photographs. The majority of the 117 million faces in the police datasets come from state driving licenses and ID cards. And when trying to solve a crime, gathering faces is as easy as pointing a camera at the street. People attending protests, visiting their church, or just walking by can all have their faces "dusted" without ever knowing it.

Tech isn't colourblind

That means most of the faces in the database are the innocent public, not hardened crooks, giving police forces a bigger canvas on which to make mistakes. "It's uncharted and frankly dangerous territory," said Alvaro Bedoya, who led the Georgetown report, in a statement.

And face recognition software is far from perfect. Under ideal conditions, which are rarely achieved in reality, face recognition is less accurate than fingerprint recognition, says Anil Jain of Michigan State University.

Facebook's face recognition software has made headlines for "closely approaching human-level performance", but systems dealing with grainy CCTV images are nowhere near this good. A big database of innocent people could actually make it harder to fight crime, because the software may start turning up more false matches than human investigators can check.

There are next to no regulations on how the police use this technology, or how much weight they give to its results. Face recognition's mystique is strong enough that, without guidance, officers may overvalue the software's output, and unconsciously favour evidence that matches its results.

Face recognition systems are also likely to be biased against black people. Since black people are arrested more often than white people, black faces are over-represented in the mugshot databases. This means that innocent black people are more likely to be linked to a crime by face recognition than innocent white people.

Face in the crowd

At the same time, research from 2012 has shown that commercial face recognition software is less accurate at analysing the faces of black people, women and children, compared with white men. So not only is the software likely to point the finger at a larger number of black people, it also points less accurately at black people than anyone else.

None of the four main companies selling face recognition technology – Cognitec, NEC, 3M Cogent and Morpho – are open about how their software works, or what datasets they use to train it. "They will not tell you what is the size of their database or where they get it from," says Jain. "That's all proprietary."

Not even the FBI knows what it's doing. In May this year, the US Government Accountability Office (GAO) released a report on the FBI's face recognition programme, stating the agency had not tested to see how often errors occurred. By conducting better tests, the GAO said, the FBI could be more sure that its system "provide leads that help enhance, rather than hinder, criminal investigations".

Like all forensic techniques, face recognition has the power to catch criminals police might otherwise miss. But to do so, its results must be transparent and reliable – otherwise you might as well just pick someone out of the crowd.

IV) Controversial software claims to tell personality from your face

A start-up says its face-recognition tech can identify people's personality type from photos – and spot terrorists, paedophiles and poker players in crowds

Terrorists and bingo players watch out

Lioba Schneider/plainpicture

By Sally Adee

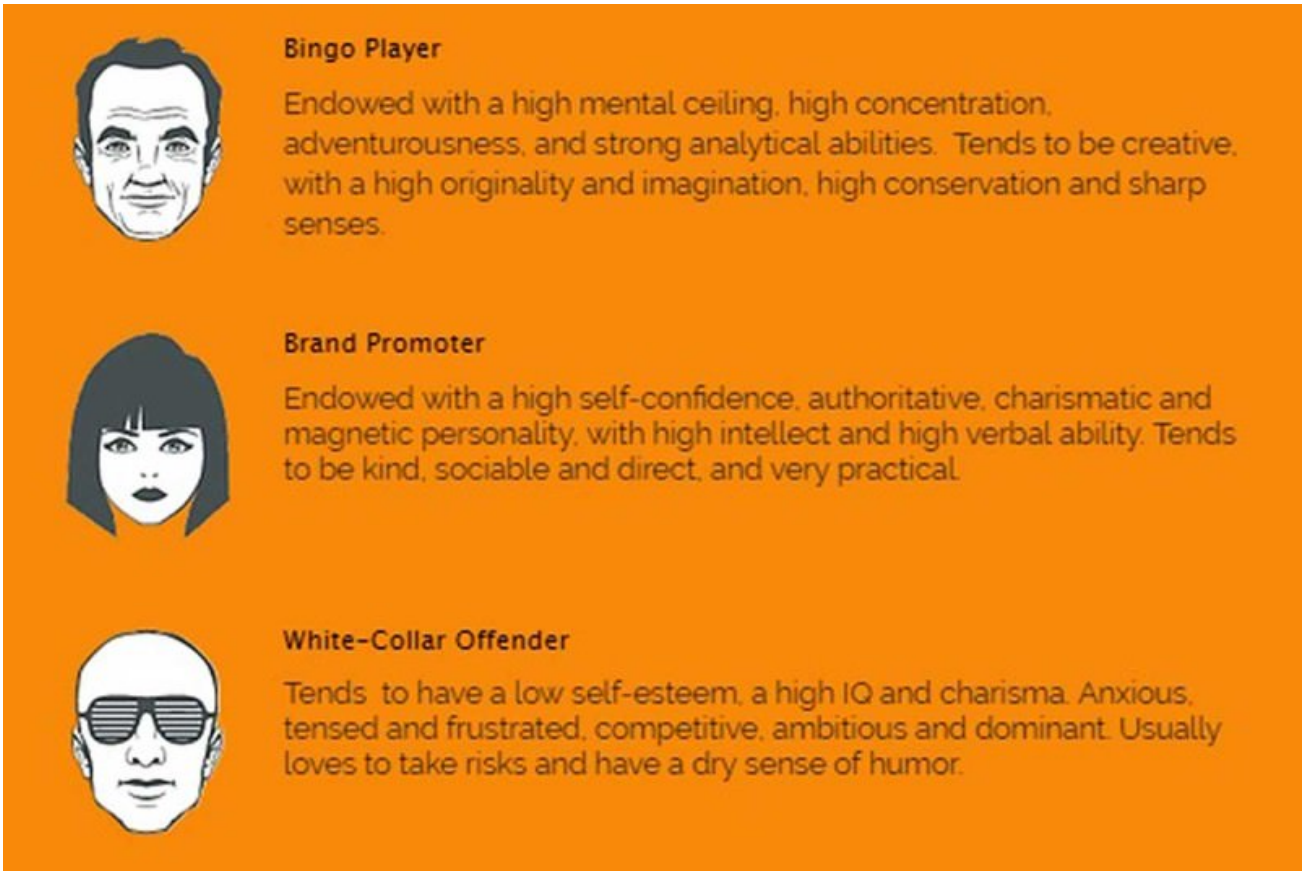
Can software identify complex personality traits simply by analysing your face? Faception, a start-up based in Tel Aviv, Israel, courted controversy this week when it claimed its tech does just that. And not just broad categories such as introvert or extrovert: Faception claims it can spot terrorists, paedophiles – and brand promoters.

Faception's algorithm scours images of a person from a variety of sources, including uploaded photos, live-streamed video and mugshots in a database. It then encodes facial features, including width and height ratio, and key points – for example, the corners of the eyes or mouth.

So far, so uncontroversial. "Using automated feature extraction is standard for face recognition and emotion recognition," says Raia Hadsell, a machine vision engineer at Google DeepMind.

.

The controversial part is what happens next. Faception maps these features onto a set of 15 proprietary "classifiers" that it has developed over the past three years. Its categories include terrorist, paedophile, white-collar criminal, poker player, bingo player and academic (see image below).



Do you see yourself here?

http://www.faception.com/

To come up with these custom archetypes, Itzik Wilf, Faception's chief technology officer, says they trained the system on the common facial features of thousands of images of known examples. The software only looks at facial features, he says, and ignores things like hairstyle and jewellery.

Wilf says this has led to notable successes. When presented with the pictures of the 11 people behind the 2016 Paris attacks, the algorithm was able to classify 9 of them as terrorists. Similarly, it spotted 25 out of the 27 poker players in an image database.

The Faception site also lists more prosaic uses for its tech, including marketing, insurance underwriting and recruiting. "HR could use it to identify suitable candidates," says Wilf.

“Faception has been working on its classifiers for more than three years now with the best team in the world to get where we are today,” says co-founder Gilad Bechar, who is now at Moburst, a marketing company in New York, but remains on the Faception board. Overall, the algorithm can class people into Faception’s categories with around 80 per cent confidence, Wilf says.

Many machine vision researchers are crying foul, however.

Arab descent?

“A classifier that tries to flag every single person of Arab descent could identify 9 out of the 11 Paris attackers at the cost of falsely flagging 370 million out of the 450 million Arabs in the world,” says Emin Gün Sirer at Cornell University in Ithaca, New York. “Such a classifier is completely useless.”

Jay Turcot, director of applied AI at emotion recognition firm Affectiva also has strong reservations. “I want to ask immediately what it says about a population that is around the same age, gender, facial hair as the Paris attackers,” he says. “How many false positives will their algorithm get? What does the test set look like?”

Wilf says that for each of their classifiers, the training sets of images run into thousands. But for behaviours as rare as terrorism or paedophilia, this will still lead to a number of false positives.

Wilf acknowledges the problem. “There are always accuracy issues with machine learning algorithms,” he says. For that reason, he says the algorithm won’t be deployed on its own and will always defer to human judgement.

However, what that would mean in practice is unclear. The algorithm apparently performs more accurately than humans do. In the past few years, physiognomy – the notion that a person’s character can be assessed from their appearance – has enjoyed a mild comeback after long being relegated to pseudoscience.

For example, differences in testosterone in men, broadly reflected in certain facial features, might lead to differences in moral decision making. But even the more recent results have been quite broad. It’s a big step from “utilitarian decision maker” to “terrorist”. What’s more, it’s not very accurate. At best, this kind of research has demonstrated “slight accuracy”, says David Perrett, who studies facial cues at the University of St. Andrews in Fife, UK. Humans can only infer personality from facial traits at a rate slightly better than chance, he says.

Shadow profiles

Face recognition technology has been at the centre of many ethics debates in recent years. Facebook was criticised for creating “shadow profiles” of people who did not have accounts of their own but appeared in images uploaded by people who did. Most recently, there was an outcry over Russian app FindFace, which scraped identifying data from social network Vkontakte so that users could identify people they snapped on the street.

“We would never license our IP to someone who would use it for those kinds of purposes,” says Wilf. But Bechar says one of its clients is an unnamed security contractor outside of the US.

“This is a new idea,” says Wilf. “New ideas are often greeted with friction.”