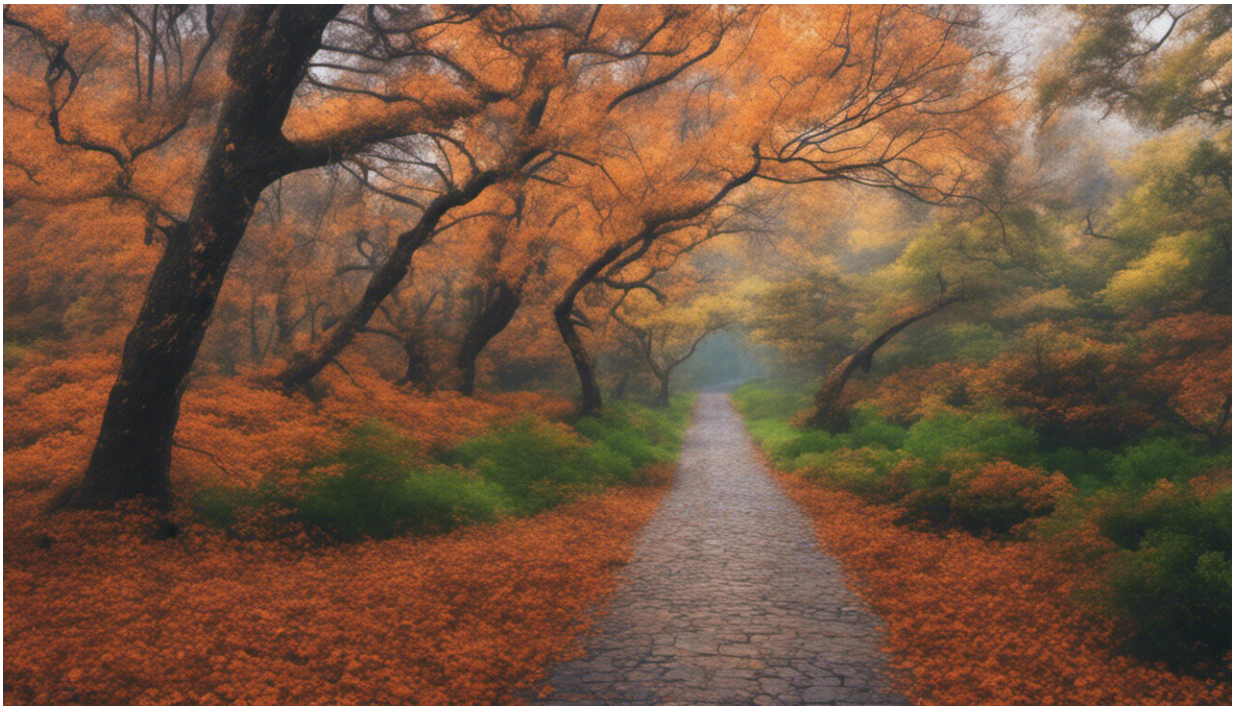
Selfies could replace security passwords – but only with an upgrade

February 23 2016, by Ian Mcloughlin, University Of Kent



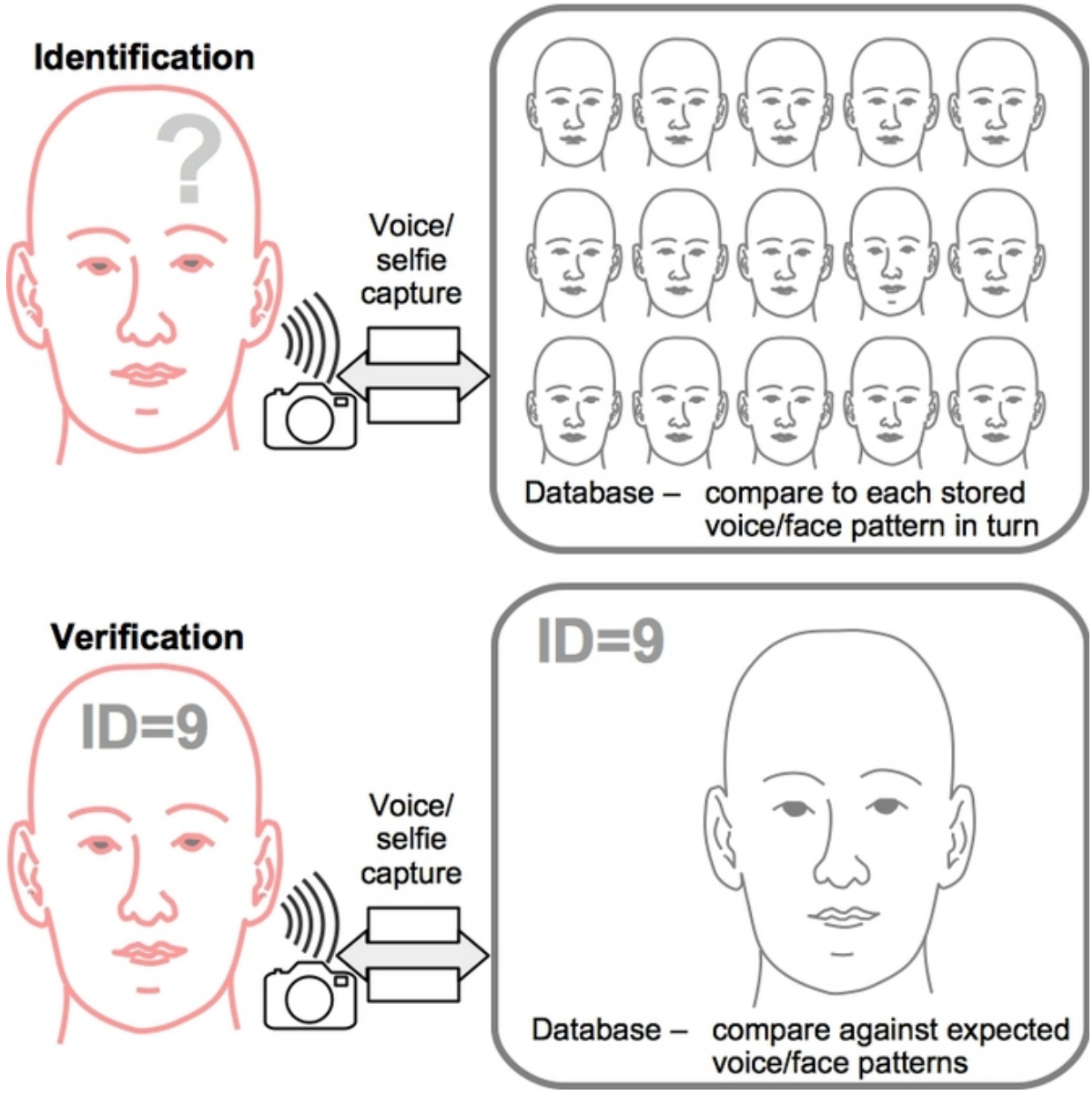
Credit: AI-generated image (disclaimer)

The next time you do some online shopping or call your bank, you may find you no longer have to scrabble around to remember your security password. Banks are increasingly turning to voice recognition technology as their preferred way of ensuring customers are who they say they are when they use telephone banking services. Mastercard has even

announced that it will accept fingerprints or selfies as proof of identity for online purchases.

But does this kind of technology really mean that you'll soon be able to just forget your passwords? The short answer right now is "no". Banks are adopting voice recognition technologies (often known as "speaker identification" in research literature) and face recognition primarily for verification, not identification. These technologies are a reasonable tool for verifying a person is who they claim to be because machines can learn how one person normally speaks or looks. But they are not yet good methods of identifying a single customer from the very large number of possible voices or faces a bank might have in their database.

For voice identification to work, the difference between your voice and others' (inter-speaker variation) must always be greater than the difference between your voice now and on another occasion (intra-speaker variation). The same is true with "selfie recognition"; you need to look more like the normal you than anyone else does. In practice, this doesn't always happen. The more voices or faces a system compares, the more likely it will find two that are very similar.



Voice or selfie recognition for identification and verification.

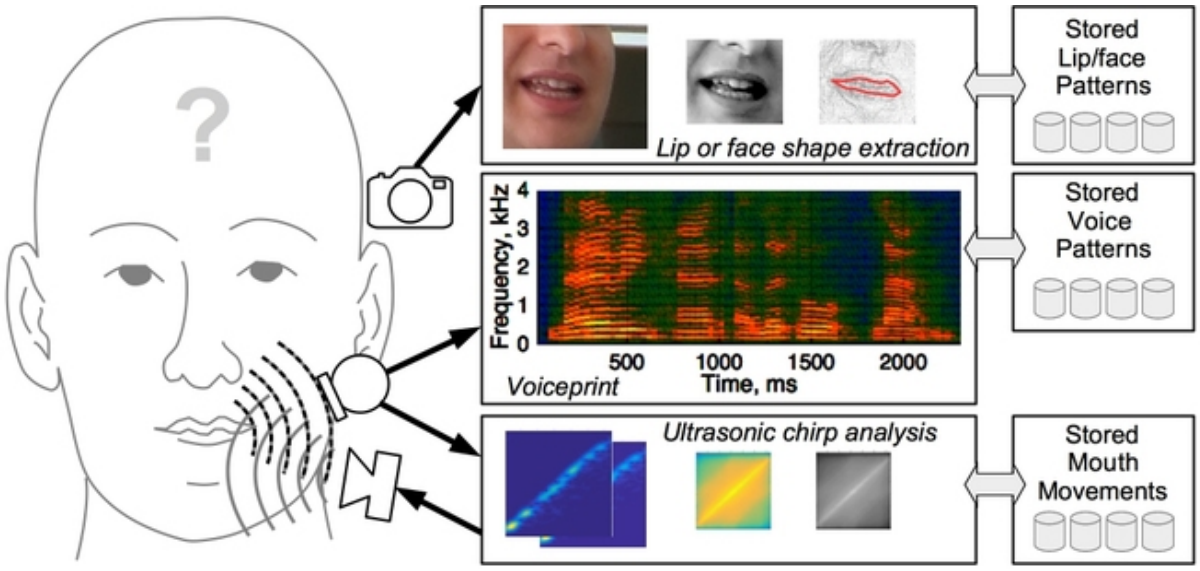
Imagine all the things that can change your own voice when you make a phone call: a blocked or damaged microphone, tiredness, mouth or throat pain, drinking excessive amounts of alcohol, eating curry or misplaced dentures. These make intra-speaker variation large. For face recognition,

facial hair, complexion changes, makeup, glasses, lighting and face coverings all contribute to changes in the way you look.

The consequence is that banks have a fair chance of "verifying" that a caller or selfie-taker is who they claim to be, but not of "identifying" an unknown voice or selfie. So we will still need a way to identify ourselves for the foreseeable future, and the best method remains a secret PIN or password.

A driver in Malaysia who had a fingerprint authentication system fitted to his new Mercedes S-class in 2005 found out the painful way that some biometrics can be stolen. When thieves discovered that his car could only be started with a fingerprint, they promptly stole his finger along with his car.

A simple voiceprint can likewise be stolen. All you need is a good quality recording of the person speaking. The same is true for systems that require a user to speak a fixed passphrase or PIN. Interactive systems using a challenge-response protocol (e.g. asking a user to repeat an unusual phrase) would raise the difficulty level for attackers, but can be defeated by current technology.



Multimodal biometric authentication.

Face recognition (such as that used to identify selfies), lip reading, and iris pattern recognition are all visual methods that could possibly be stolen or spoofed by pictures or video images.

More biometric data

The solution appears to be either making use of additional secret information (which means yet more to remember) or to combine different types of biometric information. Unfortunately, methods that require a camera are sometimes of limited use: the user must face a camera, for example, must not have glasses or clothing obscuring their face and eyes, will require adequate lighting – and the system probably should not be used while in the bath.

Other researchers are investigating the biometric potential of capturing an individual's unique brainwaves with a headset or, more recently, with

earphones. But such technology is in its infancy.

One future technology being developed for mobile devices is an ultrasound scanner that maps part of the face shape of a person speaking. This is not just a snapshot of the face, but a recording of how the mouth of the speaker moves as the words are spoken. The biometric aspect is not just confined to the sound of the voice but includes the way the mouth shape changes as the voice is produced. The required hardware is even built into most smartphones already.

Imagine walking into a bakery and picking up a crusty farmhouse loaf. You take it over to the baker and say "I would like to buy this, please." "That will be two pounds, do you wish to proceed with the purchase?" replies the baker. "Yes, please proceed," you say, and wait for their "Okay" before walking out with your loaf. No cash, no payment card and no personal details divulged.

It might sound like a scene from a bygone era when you knew your local baker and maintained an account with them. But it is, in fact, a future that researchers are working hard to enable. Your smartphone will employ voice authentication and speech recognition technology to authorise the payment with your bank who will confirm the transaction electronically with the baker. Meanwhile, a point-of-sale video recording of the transaction will be lodged with both your bank and the bakery. So while you shouldn't throw away your passwords just yet, you can expect some exciting developments in this area over the next few years.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation