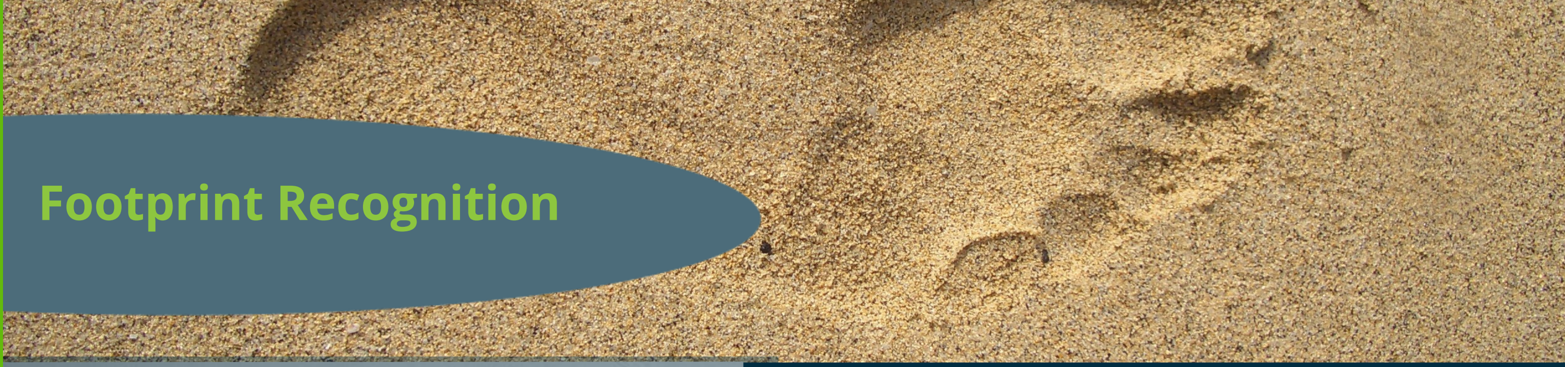
Footprint Recognition



ID FORCE International

As deepfakes increasingly threaten to overwhelm current methods of identity verification, one of the most promising means of countering them is to use multiple biometrics so that there are a variety of lines of defence. Different environments will of course require different combinations – for example online verification can, at least for the immediate future, use face, voice, and behavioural biometrics, while in the real world other physical biometrics such as iris and palm matching come into play. One of these which can work well in the right circumstances is footprint matching. f2's design covers both bare footprint and shoeprint matching. While similar, there are differences.

Footprint matching

Up to now footprint matching has been limited to academia and research labs, with, to our knowledge, no commercial products being available. However this is about to change, with our partner Canada-based Face Forensics Inc, currently working to this end.

Here's an assessment of the pros and cons of footprint matching as an aide to identity verification and identification:

Pros

- Footprint images can be easily captured – no additional hardware apart from a camera is required.
- There are sufficient differentiating features in different feet to enable them to be matched.
- Because they're almost always hidden by shoes, it's difficult for impostors to obtain someone's footprints for an attack.
- With the increasing threat from deepfakes, in the right circumstances footprints can provide an additional biometric for identification as well as identity verification.
- As the soles of a person's feet (particularly the toe patterns) can be quite different, using the soles of both feet requires little more effort and can significantly increase their value as a biometric.

Cons

- Foot matching is more intrusive and time-consuming than other biometrics as footwear has to be removed and put on again.
- All probe and database images will have to be normalised, i.e. all controllable features will have to be as similar as possible, including the direction in which the feet are pointing, the shot being taken at a right angle to the base of the foot, distance of the camera from the foot, controlled lighting, etc. In other words similar to the constraints required for passport and drivers licence photos.

Matching Images of Bare Feet

At first sight bare feet don't appear to be a particularly practical biometric, largely because during waking hours the owner will almost always be wearing shoes of some sort, and therefore the soles of the feet are rarely visible. However this is also a significant asset, as it means that those wishing to copy the footprint for their own nefarious purposes will find this extremely difficult.

Processing of the images is similar to other biometrics, i.e. the key characteristics of a foot in a photo will be encoded using f2's proprietary algorithms and then transformed into a unique digital string. This string is stored in a database for subsequent searching. When conducting identity verification, i.e. a 1:1 match, the string generated from an unidentified foot will be compared the string for the foot of the same person in the database. For identification the string will be compared with all the encodings in the database. The top matches above a user-defined threshold will be displayed for investigators to confirm if any of them match. As the database records include the name and personal details of the owner, they will have what they need to investigate the individual in detail.

A key differentiating feature of adult feet is the position of the toes. Because in many cases shoes taper towards the toes they get compressed, causing over and underlapping, as well as changing the shape of the toes themselves. This means that the footprint can reflect a wide variety of toe patterns.

Matching images of shod feet

While at first glance this may appear to be similar, there are different issues to be addressed. While the imprint of a shoe will generally be clearer than a bare foot, in the case of business shoes for example, both the sole and heel are likely to be of leather or hard rubber with no distinguishing features, leaving only the shape to work with. If the image is clear, all imprints of that model and size of shoe will match. While this may appear to be of limited use, it may be a print from the same shoe from a previous crime by the same offender. In addition, there may be cuts or marks on the original shoe which are still visible. When the investigator visually compares the probe and database images other similarities may become apparent, for example if the offender walks on the outside of his foot, the wear pattern on the sole and heel will be distinct. So while f2 Footprint may detect this and highlight the possible match, the investigator may well be able to confirm it in a visual match. The benefit of f2 Footprint in this case is that it narrows down a large number of possibilities to a few for the investigator to confirm visually.

F2 Experience in the area of Imprecise Image Matching

Some time back F2 were awarded a major contract by the UK National Crime Squad (now the NCA) to develop the ability to process images of child sexual abuse seized from suspected pedophiles. The challenge was that they would exchange these images with each other and include new images that they'd taken themselves. This resulted in seizures being comprised of a very high percentage of previously seen images, with only a relatively small number of new ones. As there's no way to separate the new images from the previously seen ones, they all had to be processed. In many cases the volumes of seized images were in the hundreds of thousands or even millions, largely because every time an exchange took place an immense number of further copies of the same images would be included. They all had to be manually viewed, requiring an enormous number of man-hours and associated trauma. Pedophiles know that copies can be identified and rejected using well-established hashing techniques which match pixel patterns, so they use automatic pixelation editors to randomly change some pixels around the edges, so that hashing algorithms wouldn't find the matches.

For the National Crime Squad we developed a method to identify these close but not identical images so investigators could focus just on them, saving an immense amount of time and investigator trauma. This worked well. Nobody else, including Microsoft, was able to produce anything like this.

Our f2 matching technology has the unique capability to match partial faces, tattoos, and scenes. This will also apply to partial footprints.

While images of the soles of feet can be found on the web, there are not a large number of these, so what's needed now is to find a source of these which can be used to create a sufficiently large database for testing purposes. One possible source could be members of the military.

Footprint matching, and object matching generally, is handled within the f2 Scene module.

Next Steps

This is to source or create the above large test database. Where applicable, this should include examples from the major different ethnic groups likely to be encountered.