Haven't I seen your face before?

Author : Cat

Date : January 22, 2014

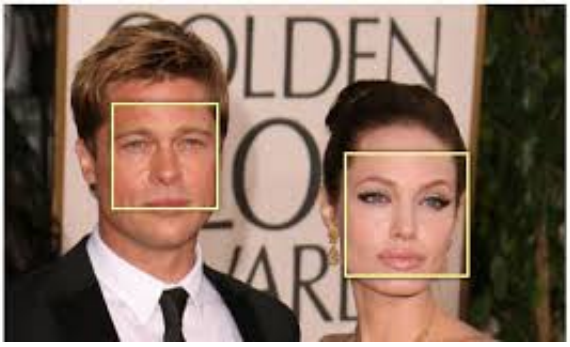
Almost every crime drama has the same scene in it - the FBI has some grainy photo of what 'might' be a suspect and then they enhance it a few times and *voila*, they have the criminal on tape! If only it were that simple.

Though the technology has come a long way, using facial recognition in a public video is still tricky. One cannot magnify a video beyond the resolution limit of the camera, the lens and the stored image. For facial recognition to work, you really need a head-on shot at high resolution. If only we had access to millions of public photos then we could compare them and at least link names to those photos. Thanks to social networks, and the accessibility of the cloud, now we do.

Who is using the technology?

Once used only for security reasons, facial recognition has become the next big thing in correlating your data. Companies can, and do, store piles of information associated to your name, email address and public profiles. This will also include any public photos you have (ie every public profile shot you have ever posted).

- **Personal Use:** iPhoto, a photo organization software, allows you to tag people in your photos and attach names to the faces. After it has a handful of names, it runs a simple algorithm on the face characteristics and will begin to suggest future tags to new photos. I find this very useful to organize a huge set of photos, by person, on my home computer, BUT the information stays there.
- **Social Networks:** This same technology is used to help identify your friends in your posted photos (only available in the US). Facebook can suggest tagging a friend based on other photos it has of that person that you have tagged. The catch here is that if the photo is public then so is the tag. If you are tagged, now that photo too has been added to your 'file'.
- **Commercial Apps:** Enter in the next generation of use, NameTag. This app is currently in beta with Google glass. Rather than entering in a still photo and comparing it against a database, NameTag allows you to look at the person in real-time and retrieve the same data. As mentioned above, you still need a clear and close, heads-on image, but it means someone could potentially glance at you through Google Glass and then be presented all your public data without you even knowing. The app company touts this as a great way to meet interesting people but others might view this as a huge breach of privacy. NameTag's database is Opt Out, which means once the service is running, you will need to go to their site to have yourself removed. They currently have 12.5 million public photos.
- **Government:** This is not a secret. They have access to photos from passports, driver's licences and criminal mug shots. At least that database is not available outside government use. Some countries have started using facial recognition for border crossing. This works because of the photos on file and the cooperative subject who positions themselves at the right angle and lighting for facial match.

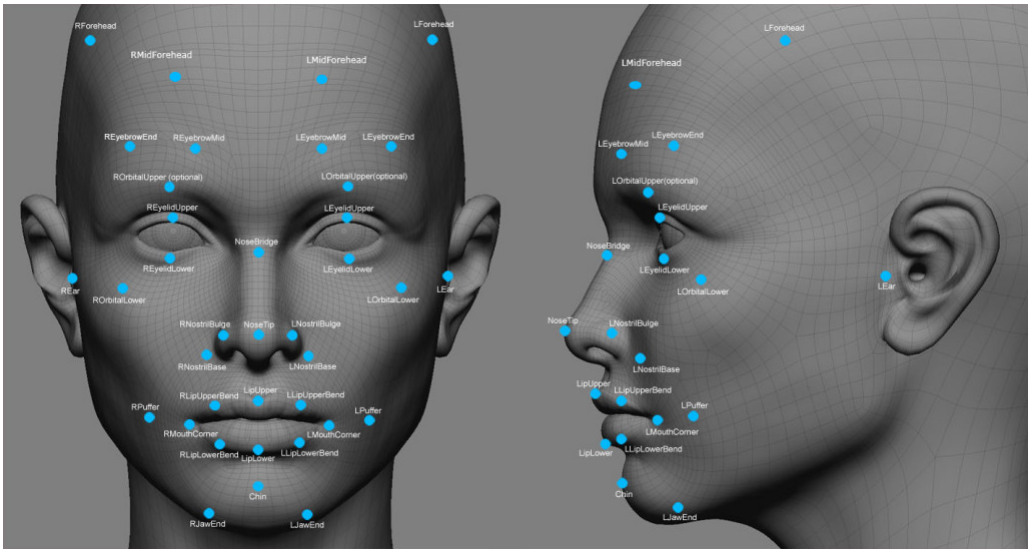


How it works

There are two parts to the process; Facial Detection and Facial Recognition. To detect a face the software looks for major facial features (eyes, nose, mouth) and the shadows that surround them. This simple algorithm exists in many digital cameras today. To deter this detection, you need only obscure a facial feature. This could be done by wearing sun glasses, a face mask or by having hair dangling over your face.

Now that we have a face, we need to determine its specific characteristics for recognition. This is called a **Faceprint**. A more sophisticated software might measure over 100 points on a face. The simplest needs the following 5:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line



There are a handful of algorithms that the software can now use to attempt to find your face in a sea of others. Clearly the more data it is has, the better the chances of making a match. Newer technologies include *3D matching* for greater angles and profiles, as well as *facial textures* to capture identifiable skin imperfections and marks.

Accuracy

For video, the best recognition software is currently used by casinos and their success rate is still

only 60-70% for a match. The problem is that you need to capture the face in the right light so that all features are available. The face also needs to be at most 20 degrees from centre, unless your reference database also includes profile shots or 3D images. For still images, the accuracy is higher, closer to 80-90%.

A good example of where this failed in video is in the hunt for the Boston Marathon Bombers in 2013. Despite having images of both suspects in their database, law agencies could not match the faces because the cell phone and surveillance footage of the scene was too grainy and not close enough to the suspects' faces.

Privacy Laws

Aye, there's the rub. There are no privacy laws specific to facial recognition... yet. Senator Al Franken was appointed as Chairman of the newly formed Judiciary Subcommittee on Privacy, Technology and the Law in the US. He has been cited in the media trying to draw attention to the issue. He has been petitioning that we put laws in place *before* the technology gets out of hand. There are currently no rules prohibiting public filming and the public information the software returns is, well, public.

What should you do?

Be aware!

- All your profile photos are public. Even if you take it down later, a copy may have already been grabbed and saved somewhere. Consider those photos carefully.
- Do not hesitate to untag yourself from public photos.
- Be wary of using kids in your profile photos. They will get filed as you and attached to your profile name. If the software gets clever enough, it could determine that the little face is not yours but belongs with you. Either way, it is now a public photo.
- Watch out for your underage kids on networks. If the network believes they are 18 then their profiles photos are fair game to be stored and searchable by many companies for these databases.
- Review your public information on sites. If Facebook knows your hometown and birthday then a stranger could approach you and say "hey, didn't you go to John Doe Highschool in 1992?", even though they have never met you.

We may not yet be walking around in world of Minority Report (2054) or Total Recall (2020), but perhaps we are closer than we think?