Biometrics

By Alia Hassan and Ingy Nazif

900131729 900131781

Computer Science Research Paper, December 2013
Biometrics

Introduction

As technology evolves, and our personal details become more and more susceptible to hacking, one of the most important concerns we now have is being sure our phones, computers, networks are secure. We have begun to move on from simple password and motion patterns onto using facial recognition, and other forms of biometric recognition technology to protect our private information. The iPhone 5 for example, now presents features to identify uniquely the owner of the device, in the form of fingerprint detection. So we decided to focus on the topic biometrics for this research paper, which is basically how to identify an individual based on his characteristics.

1- What is biometrics?

Literally, biometrics are “life measurement”, but this term is actually associated with behavioral or biological measurements. There are two main types of biometric systems: systems for identification (usually used for identifying people in a crowd using a security camera, this system is usually against the person’s consent) and for authentication (to verify a user or employee’s identity to grant him access to a place or to data).

The main concepts for choosing biometric characteristics are:

- Universal in the sense that any individual must possess this trait. This trait should be exposed the least possible to damage due to disease or accidents.
- Unchanging, the attributes should not be subject to change due to age, or environment, and should be the same for a very long period of time.
- Measurement and reducibility, the data concerning the attributes should be easy to gather and transform into an easily handled file. Moreover, the data should be easy to compare to other samples of biometric data.
- Singular and inimitable, the characteristics need to be unique to every person and impossible to reproduce or imitate.
Privacy, the use of biometrics should not violate the person's privacy.

The biometric process can be divided into two major phases: preparing the database, and the verification. The first phase is the gathering of information of the users of potential biometric based technology. The second is comparing the given data during usage to the database to match the user’s identity to a file in the database.

2- Fingerprint scanning

Fingerprints are very popular in biometrics, for the simple reason that they are unique to each person. Even identical twins have different fingerprints, and this is because fingerprints are formed during the early stages of the embryo by the amniotic fluid, which is the fluid surrounding the future baby’s skin. Our fingerprints are composed of ridges and valleys, the ridges forms discontinuities and bifurcations called “minutiae” which are used to differentiate between fingerprints.

There are different methods to gather information about fingerprints; the most common methods are optical scanning and capacitive scanning.

Optical scanners identify the reflection of light, the device takes a picture of the thumbprint and creates an inverted image and places the focus on the valleys. The capacitance scanner uses electrical current to determine where the ridges are. In fact, the ridges are non-conductive whereas the valleys are conductive. The sensor in the iPhone 5S is a capacitance scanner. These scanners are practical since they are very compact, and are very precise, it is capable of reading at 500 ppi (pixels per inch).

However, for both methods, the scanners do not compare the whole images, this would be impractical. But they compare minutiae, and certain scanners translate the image into a binary
file for the sake of privacy. Of course, it is impossible to recreate the image of the fingerprint from the binary file.

3- Retinal scanning

Retinal scanning is one of the most well-known methods of biometric identification, but it is also one of the least used. The basic concept of retinal scanning is that a person’s retina, the white area around the colored iris, has a unique pattern of blood vessels, which absorb light more easily than the surrounding tissue. Because of this they can be detected easily using the proper lighting. Due to the sensitive nature of the eye, a beam of very low energy infrared light is shone onto a person’s eye when they look into the scanner. The image of the retina is captured and then a software maps the unique pattern of blood vessels. This form of biometric identification is highly reliable because of its accuracy, but a downside of it is that to configure the database, multiple readings of the same retina are required due to the accuracy of the detail needed to find matches. The same applies for reading a retina to verify it against the database; sometimes a user can be rejected because not enough detail has been scanned.

It is important to differentiate between retinal recognition and iris recognition. The retina is a layer of tissue at the back of the eye, the retina is light-sensitive, and it is what detects images. The iris on the other hand is the colorful circle around your pupil in the front of your eye.
The iris of every person has a unique random pattern, and iris scanner analyzes this pattern to determine a person’s identity. Iris scanning is extremely specific, because compared to the 60-70 reference points in fingerprint scanning, irises have up to 200 reference points that are compared to identify a person. The color, the depth and the indents are all analyzed to create a detailed picture of the iris, and then this is compared against a database.

4- Facial recognition
Scientists started to work on facial recognition technology in the 1960s, since then it has advanced a lot. Facial recognition technology used to be based on whole images being compared, which made the matching very imprecise.

Nowadays, this technology is based on the measurement of ‘nodal points’, points and distances that are unique and unchanging in each and every individual (distance between the eyes, form of cheekbones, etc.). After taking the measurement the program creates a numerical code for the face, the ‘faceprint’. Another recent advancement in the same field is Surface Texture Analysis, which basically follows a similar process but creates a skinprint, and can differentiate between the skins of two identical twins.

Currently, most facial recognition software go through three steps using three templates to identify or verify the identity of a subject: vector template, local feature analysis, and surface texture analysis. The first, is used to quickly search for a set of possibly matching faces. The second, refines the set of possible matches through a secondary search. The third, which uses the more, detailed template, and relies on the skin features.

The combination of the three searches makes the matching possible in disregard of the facial expression of the subject. Nonetheless, some things can alter the matching and the accuracy of this system such as: wearing sunglasses, having long hair hiding the center of the face or if the subject is too far from the camera.

5- Voice recognition

It is very important to differentiate between voice recognition and speech recognition. Voice recognition, can also be called speaker recognition: defining who is speaking, it is not defining the words that are spoken, that is speech recognition. Voice recognition can be used to identify a speaker, and also to authenticate a speaker. This biometric authentication method is based on the unique acoustic patterns that each person has, as these patterns reflect in them, both the anatomy of the speaker (the size of the mouth and throat etc.) and their behavioral patterns (their way of speaking, pitch etc.).

The way it works is a speaker will say a few words, and they will be recorded, and using an analogue-to-digital converter they will be converted to digital signals. Various aspects of the
speaker’s voice are analyzed such as the frequency and the volume and the pitch. Comparing these pieces of information, as well as other more technical information, to a database the software can find the speaker’s identity, and see if they are allowed access to the information they seek.

6- What is ‘biometrisable’ and concerns about biometrics:

Something that is ‘biometrisable’ is a trait that is unique to a person that can be somehow used to identify them from others. Many features in a person could be ‘biometrisable’, other than the ones mentioned above, such as ears, gait (the way a person walks), odor, footprints, lips, teeth and also the obvious features of blood and DNA. But most are impractical, gait for example isn’t a stable feature, and teeth are difficult to get access to, so for now they are mainly used as a method of post-mortem identification. These other forms of biometrics are not used commercially because of issues such as hygiene and inconvenience, for the lip prints for example, they are in fact as unique as fingerprints, and lip shaped as specific to each individual, but there is the hygienic issue of making repeated lip prints for different people on the same machine. Once this is solved, they can become more popular.

Some concerns about biometrics are that: firstly, people may become so reliant on biometrics and believe them to be so reliable that they begin to neglect taking normal security measures to protect their data. There is the issue of minority populations for whom some biometric systems cannot be adapted, such as the elderly and the disabled. In terms of emergency situations, since different biometrics companies probably use different variations of the basic recognition processes, they will each have slightly varied databases, and so if in the case of emergency, these databases need to be compared, there could be a delay in data transfer and this could harm the situation.

Biometrics are an easy way to not have to carry a key, remember a password and so on. But what is more harmful, a stolen key or a stolen eye or finger? The fact that makes biometrics safer and more dangerous is that it relies on the fact that it is unique for each and every one of us. In other words, the only way to break through a biometric system is to actually steal a part of the body. This is why companies are now working to be able to differentiate between dead and living parts of the bodies as well. We see illustrations of this danger in books like “Angels &
Demons”, by Dan Brown, in which the criminal steals the physicist’s eye to fool the iris recognition system and enter a restricted place.

Conclusion

Biometrics is a process that is evolving rapidly because of the security concerns we face. It would be easier for policemen to identify a criminal through a by using a security camera and searching through a database. Biometrics is used for identification and verification. Some high-tech companies use iris scanning or fingerprints scanning to uniquely identify an individual. The concept of biometrics is meant to make it easier to protect our private information, but a side effect is that we may become careless in actively protecting our data, assuming that biometrics are fool-proof. On one hand, the system can turn out to be inaccurate in certain conditions, if the face axis rotation is turned more than 90 degrees away from the camera, etc. On the other hand, aren’t biometrics encouraging more violent crimes by making the key a part of our body? And how about privacy? Is it ethical to tape every single movement of every single person’s life? Could these images fall into unworthy and unethical hands?
Works Cited


