How Facial Recognition Systems Work

by Kevin Bonsor

A ticket to **Super Bowl XXXV** in Tampa Bay, Florida, didn't just get you a seat at the biggest professional football game of the year. Those who attended the January 2000 event were also part of the largest police lineup ever conducted, although they may not have been aware of it at the time. The Tampa Police Department was testing out a new technology, called FaceIt, that allows snapshots of faces from the crowd to be compared to a database of criminal mugshots.

Photo courtesy Visionics

Facial recognition software can be used to find criminals in a crowd, turning a mass of people into a big lineup.

The $30,000 system was loaned to the Tampa Police Department for one year. So far, no arrests have been made using the technology. However, the 36 cameras positioned in different areas of downtown Tampa have allowed police to keep a more watchful eye on general activities. This increased surveillance of city residents and tourists has riled privacy rights groups.

People have an amazing ability to recognize and remember thousands of faces. In this edition of **HowStuffWorks**, you'll learn how computers are turning your face into computer code so it can be compared to thousands, if not millions, of other faces. We'll also look at how **facial recognition software** is being used in elections, criminal investigations and to secure your personal computer.

The Face

Your face is an important part of who you are and how people identify you. Imagine how hard it would be to recognize an individual if all faces looked the same. Except in the case of identical twins, the face is arguably a person's most unique physical characteristic. While humans have had the innate ability to recognize and distinguish different faces for millions of years, computers are just now catching up.

Visionics, a company based in New Jersey, is one of many developers of facial recognition technology. The twist to its particular software, **FaceIt**, is that it can pick someone's face out of a crowd, extract that face from the rest of the scene and compare it to a database full of stored images. In order for this software to work, it has to know what a basic face looks like. Facial recognition software is based on the ability to first recognize faces, which is a technological feat in itself, and then measure the various features of each face.

Photo courtesy Visionics

Facial recognition software is designed to pinpoint a face and measure its features.

If you look in the mirror, you can see that your face has certain distinguishable landmarks. These are the peaks and valleys that make up the different facial features. Visionics defines these landmarks as **nodal points**. There are about 80 nodal points on a human face. Here are a few of the nodal points that are measured by the software:

- **Distance between eyes**
- **Width of nose**
- **Depth of eye sockets**
- **Cheekbones**
- **Jaw line**
- **Chin**

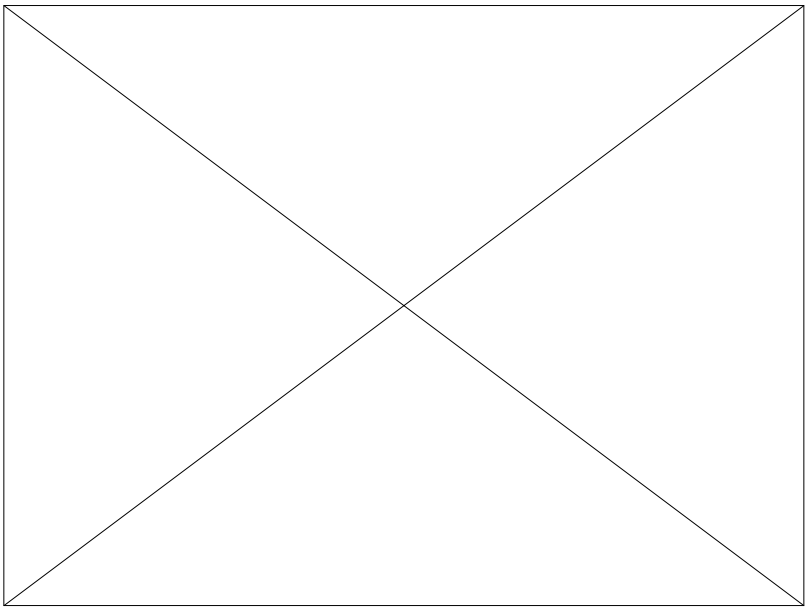
These nodal points are measured to create a numerical code, a string of numbers, that represents the face in a database. This code is called a **faceprint**. Only 14 to 22 nodal points are needed for the FaceIt software to complete the recognition process. In the next section, we'll look at how the system goes about detecting, capturing and storing faces.

The Software

Facial recognition software falls into a larger group of technologies known as **biometrics**. Biometrics uses biological information to verify identity. The basic idea behind biometrics is that our bodies contain unique properties that can be used to distinguish us from others. Besides facial recognition, biometric authentication methods also include:

- **Fingerprint scan**
- **Retina scan**
- **Voice identification**

Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze and compare your face to a database of stored images. Here is the basic process that is used by the FaceIt system to capture and compare images:



To identify someone, facial recognition software compares newly captured images to databases of stored images.

1. **Detection** - When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A **multi-scale algorithm** is used to search for faces in low resolution. (An algorithm is a program that provides a set of instructions to accomplish a specific task). The system switches to a high-resolution search only after a head-like shape is detected.
2. **Alignment** - Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least **35 degrees** toward the camera for the system to register it.
3. **Normalization** -The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera. Light does not impact the normalization process.
4. **Representation** - The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.
5. **Matching** - The newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation.

The heart of the FaceIt facial recognition system is the **Local Feature Analysis** (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a **faceprint**, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of faceprints stored in a database. Each faceprint is stored as an **84-byte file**.

Photo courtesy Visionics

Using facial recognition software, police can zoom in with cameras and take a snapshot of a face.

The system can match multiple faceprints at a rate of 60 million per minute from memory or 15 million per minute from hard disk. As comparisons are made, the system assigns a value to the comparison using a scale of one to 10. If a score is above a predetermined threshold, a **match** is declared. The operator then views the two photos that have been declared a match to be certain that the computer is accurate.

Facial recognition, like other forms of biometrics, is considered a technology that will have many uses in the near future. In the next section, we will look how it is being used right now.

Gotcha!

The primary users of facial recognition software like FaceIt have been law enforcement agencies, which use the system to capture random faces in crowds. These faces are compared to a database of criminal mug shots. In addition to law enforcement and security surveillance, facial recognition software has several other uses, including:

- **Eliminating voter fraud**
- **Check-cashing identity verification**
- **Computer security**

One of the most innovative uses of facial recognition is being employed by the Mexican government, which is using the technology to weed out duplicate voter registrations. To sway an election, people will register several times under different names so they can vote more than once. Conventional methods have not been very successful at catching these people.

Using the facial recognition technology, officials can search through facial images in the voter

database for duplicates at the time of registration. New images are compared to the records already on file to catch those who attempt to register under aliases. The technology was used in the country's 2000 presidential election and is expected to be used in local elections soon.

Potential applications even include ATM and check-cashing security. The software is able to quickly verify a customer's face. After the user consents, the ATM or check-cashing kiosk captures a digital photo of the customer. The FaceIt software then generates a faceprint of the photograph to protect customers against identity theft and fraudulent transactions. By using facial recognition software, there's no need for a picture ID, bank card or personal identification number (PIN) to verify a customer's identity.

Photo courtesy Visionics

Many people who don't use banks use check cashing machines. Facial recognition could eliminate possible criminal activity.

This biometric technology could also be used to secure your computer files. By mounting a Webcam to your computer and installing the facial recognition software, your face can become the password you use to get into your computer. IBM has incorporated the technology into a screensaver for its A,T and X series Thinkpad laptops.

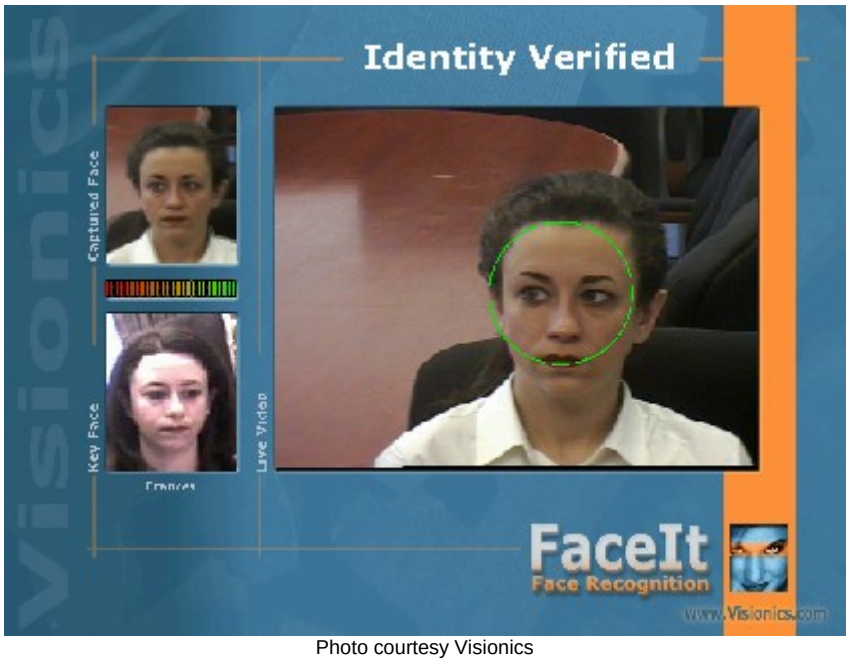


Photo courtesy Visionics

Facial recognition software can be used to lock your computer.

While facial recognition can be used to protect your private information, it can just as easily be used to invade your privacy by taking you picture when you are entirely unaware of the camera. As with many developing technologies, the incredible potential of facial recognition comes with drawbacks.