How Facial Recognition Systems Work (adapted from howstuffworks.com)

Anyone who has seen the TV show "Las Vegas" has seen facial recognition software in action. But what looks so easy on TV doesn't always translate as well in the real world.

In 2001, the Tampa Police Department installed cameras equipped with facial recognition technology in their Ybor City nightlife district in an attempt to cut down on crime in the area. The system failed to do the job, and it was scrapped in 2003 due to ineffectiveness. People in the area were seen wearing masks and making obscene gestures, prohibiting the cameras from getting a clear enough shot to identify anyone.

Boston's Logan Airport also ran two separate tests of facial recognition systems at its security checkpoints using volunteers. Over a three month period, the results were disappointing. According to the Electronic Privacy Information Center, the system only had a 61.4 percent accuracy rate, leading airport officials to pursue other security options.

Humans have always had the innate ability to recognize and distinguish between faces, yet computers only recently have shown the same ability. In the mid 1960s, scientists began work on using the computer to recognize human faces. Since then, facial recognition software has come a long way.

Identix®, a company based in Minnesota, is one of many developers of facial recognition technology. Its software, FaceIt®, can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images. In order for this software to work, it has to know how to differentiate between a basic face and the rest of the background. Facial recognition software is based on the ability to recognize a face and then measure the various features of the face.

Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. FaceIt defines these landmarks as nodal points. Each human face has approximately 80 nodal points. Some of these measured by the software are:

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

These nodal points are measured creating a numerical code, called a faceprint, representing the face in the database.
In the past, facial recognition software has relied on a 2D image to compare or identify another 2D image from the database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. This created quite a problem.

In most instances the images were not taken in a controlled environment. Even the smallest changes in light or orientation could reduce the effectiveness of the system, so they couldn't be matched to any face in the database, leading to a high rate of failure. In the next section, we will look at ways to correct the problem.

**3D Facial Recognition**

A newly-emerging trend in facial recognition software uses a 3D model, which claims to provide more accuracy. Capturing a real-time 3D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time.

Using depth and an axis of measurement that is not affected by lighting, 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile).

Using the 3D software, the system goes through a series of steps to verify the identity of an individual.

**Detection**

Acquiring an image can be accomplished by digitally scanning an existing photograph (2D) or by using a video image to acquire a live picture of a subject (3D).

**Alignment**

Once it detects a face, the system determines the head's position, size and pose. As stated earlier, the subject has the potential to be recognized up to 90 degrees, while with 2D, the head must be turned at least 35 degrees toward the camera.
Measurement
The system then measures the curves of the face on a sub-millimeter (or microwave) scale and creates a template.

Representation
The system translates the template into a unique code. This coding gives each template a set of numbers to represent the features on a subject's face.

Matching
If the image is 3D and the database contains 3D images, then matching will take place without any changes being made to the image. However, there is a challenge currently facing databases that are still in 2D images. 3D provides a live, moving variable subject being compared to a flat, stable image. New technology is addressing this challenge. When a 3D image is taken, different points (usually three) are identified. For example, the outside of the eye, the inside of the eye and the tip of the nose will be pulled out and measured. Once those measurements are in place, an algorithm (a step-by-step procedure) will be applied to the image to convert it to a 2D image. After conversion, the software will then compare the image with the 2D images in the database to find a potential match.

Verification or Identification
In verification, an image is matched to only one image in the database (1:1). For example, an image taken of a subject may be matched to an image in the Department of Motor Vehicles database to verify the subject is who he says he is. If identification is the goal, then the image is compared to all images in the database resulting in a score for each potential match (1:N). In this instance, you may take an image and compare it to a database of mug shots to identify who the subject is.

Surface Texture Analysis

The image may not always be verified or identified in facial recognition alone. Identix® has created a new product to help with precision. The development of FaceIt®Argus uses skin biometrics, the uniqueness of skin texture, to yield even more accurate results. The process, called Surface Texture Analysis, works much the same way facial recognition does. A picture is taken of a patch of skin, called a skinprint. That patch is then broken up into smaller blocks. Using algorithms to turn the patch into a mathematical, measurable space, the system will then distinguish any lines, pores and the actual skin texture. It can identify differences between identical twins, which is not yet possible using facial recognition software alone. According to Identix, by combining facial recognition with surface texture analysis, accurate identification can increase by 20 to 25 percent.

FaceIt currently uses three different templates to confirm or identify the subject: vector, local feature analysis and surface texture analysis.

By combining all three templates, FaceIt® has an advantage over other systems. It is relatively insensitive to changes in expression, including blinking, frowning or smiling and has the ability to compensate for mustache or beard growth and the appearance of eyeglasses. The system is also uniform with respect to race and gender. However, it is not a perfect system. There are some factors that could get in the way of recognition, including:
- Significant glare on eyeglasses or wearing sunglasses
- Long hair obscuring the central part of the face
- Poor lighting that would cause the face to be over- or under-exposed
- Lack of resolution (image was taken too far away)

Identix isn’t the only company with facial recognition systems available. While most work the same way Facelt does, there are some variations. For example, a company called Animetrix, Inc. has a product called FACEngine ID® SetLight that can correct lighting conditions that cannot normally be used, reducing the risk of false matches. Sensible Vision, Inc. has a product that can secure a computer using facial recognition. The computer will only power on and stay accessible as long as the correct user is in front of the screen. Once the user moves out of the line of sight, the computer is automatically secured from other users.

**Current and Future Uses of Facial Recognition Systems**

In the past, the primary users of facial recognition software have been law enforcement agencies, who used the system to capture random faces in crowds. Some government agencies have also been using the systems for security and to eliminate voter fraud. The U.S. government has recently begun a program called **US-VISIT** (United States Visitor and Immigrant Status Indicator Technology), aimed at foreign travelers gaining entry to the United States. When a foreign traveler receives his visa, he will submit fingerprints and have his photograph taken. The fingerprints and photograph are checked against a database of known criminals and suspected terrorists. When the traveler arrives in the United States at the port of entry, those same fingerprints and photographs will be used to verify that the person who received the visa is the same person attempting to gain entry.

However, there are now many more situations where the software is becoming popular. As the systems become less expensive, making their use more widespread. They are now compatible with cameras and computers that are already in use by banks and airports. The TSA is currently working on and testing out its Registered Traveler program. The program will provide speedy security screening for passengers who volunteer information and complete a security threat assessment. At the airport there will be specific lines for the Registered Traveler to go through that will move more quickly, verifying the traveler by their facial features.

Other potential applications include ATM and check-cashing security. The software is able to quickly verify a customer’s face. After a customer consents, the ATM or check-cashing kiosk captures a digital image of him. The Facelt software then generates a faceprint of the photograph to protect customers against identity theft and fraudulent transactions. By using the facial recognition software, there’s no need for a picture ID, bankcard or personal identification number (PIN) to verify a customer's identity. This way businesses can prevent fraud from occurring.

**Time Tracking**

**A4Vision**, a creator of facial recognition software, is currently marketing a system that will keep track of employees' time and attendance. Their website states that it will prohibit "buddy punching," which will cut down on security risks and decreased productivity.
While all the examples above work with the permission of the individual, not all systems are used with your knowledge. In the first section we mentioned that systems were used during the Super Bowl by the Tampa Police, and in Ybor City. These systems were taking pictures of all visitors without their knowledge or their permission. Opponents of the systems note that while they do provide security in some instances, it is not enough to override a sense of liberty and freedom. Many feel that privacy infringement is too great with the use of these systems, but their concerns don’t end there. They also point out the risk involved with identity theft. Even facial recognition corporations admit that the more use the technology gets, the higher the likelihood of identity theft or fraud.

As with many developing technologies, the incredible potential of facial recognition comes with some drawbacks, but manufacturers are striving to enhance the usability and accuracy of the systems.

QUESTIONS:

1. What is a ‘faceprint’?
2. What are the problems in 2D face recognition systems?
3. What makes 3D facial recognition system work?
4. What makes Facelt superior compared to other systems?
5. What are its problems?
6. Where is facial recognition used nowadays?
7. How will it be used in the future?

CROSSWORD PUZZLE:

Across
2. a hindrance
3. to verify
5. to improve
6. to produce
8. to make unclear or indistinct
9. a model or standard
10. a crime less serious than a felony

Down
1. main
3. can be used with other device without modification
4. to make smaller
7. you were born with it