The Science Behind Passfaces

Significant research has been conducted regarding the brain's ability to recognize faces. To a great extent the purpose of these studies has been to create electronic devices that emulate the brain. In doing so, faces could be used as identifying factors for biometric security systems. Like many functions of the brain the process is more complex than one might first think. It turns out that the brain treats face recognition differently than it does shapes and objects. It is this fact that serves as basis behind the core technology of Passfaces.

The Science

Think of Passfaces as kind of a reverse biometrics. Rather than trying to recreate the complexity of the human brain, Passfaces takes advantage of it. Studies indicate that we all have the innate ability to recognize faces long after we are first exposed to them. In short, faces are much easier to "remember" than passwords or PINS. The result is a system that uses faces as a replacement for passwords.

Passfaces is supported by extensive academic studies and experiments. Research was conducted by Professor Hadyn Ellis [1], a world authority on face recognition and Head of the School of Psychology at University of Wales Cardiff. The research[2] , which dates back to the 1970s, centered on discovering how the human visual brain works and specifically how it perceives, remembers and recognizes faces.

It is largely accepted that the brain is not just a big computer, but has many unique processes that are barely understood. The brain appears to have evolved special components to handle tasks that may have been crucial to survival. One of these is the ability to recognize faces which involves separate processes for learning a new face and subsequently recognizing it.

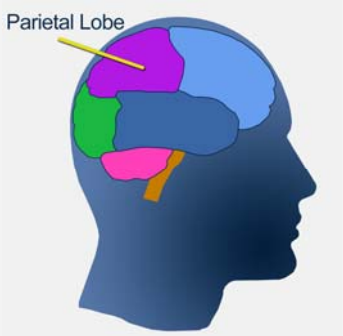
Generally the right side of the brain is concerned with pictures and spatial relationships. The left has more to do with abstract processes like mathematics and language. The right parietal lobe (right side upper middle) of the brain controls face recognition but other parts are also involved. As a comparison, passwords use the left the brain and Passfaces uses the right brain.

Face Perception

Face recognition is a dedicated process which is different from general object recognition. One of the strongest pieces of evidence to support this view is the face inversion effect where inverted faces are much harder to recognize than a normal face.[3]

Based on the Brain's Innate Ability to Recognize Faces

Passfaces can be thought of as a kind of reverse biometrics. Rather than trying to recreate the complexity of the human brain, Passfaces takes advantage of it.



The right side of the brain is concerned with pictures and spatial relationships. The right parietal lobe controls face recognition but other parts are also involved. As a comparison, passwords use left brain and Passfaces uses the right brain.

[1] Professor Hadyn Ellis School of Psychology University of Wales Cardiff
[2] The Face Recognition Home Page. www.face-rec.org
[3] Face Recognition: A literature Survey. National Institute of Standards and Technology

The Science Behind Passfaces

Both inference and direct neurological measurement indicate that our brains have a special component whose sole function is to recognize faces. Viewing and recognizing faces is not like looking at other objects. It is special as illustrated by the following:

- Infants are born with a capacity to recognize faces and show a preference for looking at faces well within the first hour after birth.
- Infants can recognize their mother after only two days.
- We know that we have seen a familiar face within twenty thousandths of a second (20ms).
- In one experiment people recognized schoolmates they had not seen for 35 years with over 90% accuracy.

This special characteristic is an important distinction of Passfaces. There are some security software products on the market that introduce picture or object recognition as an additional component of authentication. For example, one security package asks users to select a picture of a place or thing as a "security secret" to be used as an additional authentication factor to passwords. Like a password, users must remember the picture they have chosen. This is not the case with Passfaces. The human brain recognizes, not remembers, faces. This ability is unique to human faces and does not apply to other images.

It is believed that our evolutionary past plays a role in our ability to recognize faces. It was vital that we quickly recognize friend, foe or stranger. Evolution has given us a special cognometric[4] process to deal with this need. It is also believed that the brain may store faces in some sort of spatial relationship. The more distinctive a face then the fewer other faces there are like it. The face is recognized more quickly because there are more elements that are unique to it and fewer elements common to many others. These elements do not appear to be dimensions and parts of a face but more grades of texture and overall shape. Face recognition is a holistic process therefore our brains do not analyze faces into portions.

Elements Fostering Recognition are Engineered into Passfaces

Emotion Helps

One is more likely to recognize someone with a definite expression as opposed to a neutral look. People obviously prefer looking at happy pleasant faces rather than sad or menacing ones.
Passfaces uses pictures of people showing happiness in the form of a smile.

Context is Important

The context in which a person is met or recognized influences the ability to recognize them later. For example; someone you met on the beach during vacation may not be recognized later at a different location. Adults also tend to more easily recognize people whom are perceived as important to us.

The Brain Deals with Faces Differently than Any Other Image

Face recognition is a dedicated process which is different from general object recognition. One of the strongest pieces of evidence to support this view is the face inversion effect where inverted faces are much harder to recognize than a normal face. Source: Face Recognition: A Literature Survey. National Institute of Standards and Technology

Passfaces is Designed to Foster Face Recognition

Smiling, happy faces are easier to recognize because they display emotion and are pleasant to look at.

[4] Cognometric. 1. A measurable, innate cognitive ability of the human brain (e.g. ability to recognize a familiar face or musical tune). 2. Method of personal authentication based on measuring an innate cognitive ability of the human brain (e.g. ability to recognize a familiar face). [C21: from Latin cognoscere, to recognize + Greek metro, measure]

Passfaces are always presented within the same context, as a log on to a secured web site or system. Because they are used for security, the importance of Passfaces is implied.

Quality and Color

Even if image quality is poor, distorted, or of only a small number of pixels faces are still easily recognized as someone known. There is no difference between recognizing a color or black and white image. Passfaces uses lower resolution images. The quality is still good, but the reduced resolution requires a smaller file size therefore speeding the loading of images on slower Internet connections.

Repetition Priming

If you have just seen a face you will recognize it more quickly than if you had not just seen it. This process is called "repetition priming". Passfaces recommends that procedures be put in place to assure users return to their login within a week of signing up for Passfaces. This increases the retention.

Semantic Priming

If you have just seen a face that has a relationship to another you will recognize the other more quickly. This is known as "semantic priming". Seeing faces as part of a group enhances recognition when presented with that group.
A single Passface is presented with 8 decoys. Decoys are always the same thus establishing a relationship and reinforcing Semantic Priming. Seeing faces within a group helps identify the correct face because those which are not familiar are easily eliminated.

Tying a Name to a Face

Identifying to whom a face belongs is a further and somewhat different process. There appears to be no tie between faces and names, so an inability to put a name to a face is a common occurrence.
Passfaces do not require the user to identify a face - only to recognize that it is familiar. This means that the commonest area of concern - "I recognize that person but can't remember their name" - is not an issue. There is no evidence that a person's ability to recognize faces deteriorates with age. Actually, adults are better than young children at recognizing faces. There is no correlation between face recognition ability and culture, education or intelligence. It is a truly universal skill.

Applying the Technology to Passfaces

Users are assigned Passfaces much like they are assigned passwords. And just as a password requires a number of alpha numeric characters to make up the word, Passfaces requires a number of faces to make up a Passfaces Code. One way to think of Passfaces is that human faces replace the individual characters typically found in a password.

Advantages to using Passfaces over passwords include the following:

- Can’t be written down or copied
- Can’t be given to another person
- Can’t be guessed
- Involve cognitive not memory skills
- Can be used as a single or part of a dual form of authentication

Passfaces Assignment and Presentation

User are assigned a sequence of Passfaces that replace passwords or are used as a second form of authentication

Assigned Passfaces are presented to the user, one at a time, in a 3 face by 3 face grid that contains the assigned Passface and 8 decoys

The Science Behind Passfaces

The basic configuration of Passfaces is typically from 3 to 7 Passfaces that make up a single code. This number is variable depending on the application and like a password is determined by the system administrator. The number of Passfaces assigned takes into account a combination of security, usability and practicality considerations.

Each Passface is presented to the user in a grid, typically 3 faces by 3 faces, that contains the assigned Passface and 8 decoys that are similar in appearance. In theory, the grid can be any size and contain more than a single Passface. However, it has been found by experiment that having overlarge grids or more than one Passface per grid can be difficult or even confusing for the user. The 3x3 grid has an obvious advantage in that it maps directly to a numerical keypad allowing Passfaces to be used on devices such as ATMs and Web TVs where this may be the only means of user input.

Using five Passfaces picked from five 3x3 grids provides 9^5 combinations or 1 chance in 59,049 that someone could guess the Passfaces at random. This is sufficient for many consumer and business applications provided, of course, that the system is not open to exhaustive search by an attacker. For comparison, consider the four-digit user-selected PIN used globally on ATM networks. The chances of someone guessing a PIN are less than 1 in 10,000.

Higher security is achieved by using more than 5 Passfaces. There is no known limit to the number of faces that a person can remember. Passfaces can be used with another authenticator, such as a password or a token, as part of a two-factor “strong” authentication scheme.

Display Parameters

The size of the displayed images has been chosen to allow the full grid to be easily perceived (on an average-sized computer monitor) without requiring excessive head or eye movement. Our experience has shown a wide variation in how people look at the grid of faces. Some scan from left to right and top to bottom as if they were reading. Others follow a zigzag path while some spiral out from the center. Some seem to take in the whole grid with a single glance.

Passfaces images are normally color and shown in a portrait format, a very natural way of seeing people. However, showing the faces as grayscale is not detrimental to ease of recognition. Passfaces works equally well on a non-color Palm PDA device for example. Highly security-conscious security administrators may even opt for grayscale on all platforms in order to make it even harder for a user to describe their Passfaces to someone else.

In some high-security applications the grids of faces may be displayed only for a very short time. A half second is long enough for practiced users to recognize their Passfaces. Combined with masking (faces in a grid are overwritten with a common mask face) it is extremely difficult for “shoulder surfers” to learn the Passfaces as the user clicks on them. Users can also be given the option to enter the grid position of each Passfaces on a keypad, rather than picking them out on the screen.

Mouse Click or Keyboard Entry

The 3 by 3 grid gives users the ability to use their mouse to click on a Passface or a numeric keypad to enter the number that corresponds to the face on the grid.

Face Sets

Faces used are recorded especially for Passfaces with a digital movie camera. Subjects are lit primarily from above and to the right, which is a natural lighting position and shows the texture and shading of faces.
A user's set of Passfaces is chosen randomly by the system making all faces in each of the logon grids equally likely to be a possible Passface. This also makes enrolling easier since users do not have to worry about choosing faces. Contrast this with passwords where a system-selected password is difficult to remember.

The grids of faces in Passfaces are grouped by sex and are selected to be equally distinctive so that Passfaces cannot be described by gender or obvious characteristics. None of the faces stand out from the others. Only when a Passface is shown at login will it seem to stand out from the other eight "decoy" faces in the grid.

A Passface is always seen in a grid with the same eight decoys. Our experience and trials show that although the users gain a certain level of familiarity with the decoys, speed and accuracy at recognizing their Passfaces increases.

Enrollment

The Passfaces enrollment process has been optimized, through trials carried out by Professor Tim Valentine, Head of Department of Psychology at Goldsmiths College, University of London. Users typically spend 3 to 5 minutes enrolling. In that short amount of time, users are sufficiently familiarized with their Passfaces to recognize them within a week of enrollment. The trials and data analysis from the Passfaces Web site validate that users who login within two weeks of enrollment are able to reliably login again six months later, even if they have not used the system.

There are two enrollment phases: introduction and practice. During introduction, individual Passfaces are shown to the user. Users then practice picking out each Passface from grids of nine faces. In order to complete enrollment, users must get through at least four iterations of practice without picking a decoy. Prompts are provided during the first couple of practice phases.

Final Points

Passfaces is specifically designed to take advantage of the brain's natural ability to recognize faces. The system only works with faces and not other objects. Any organization may choose to have a custom set of faces created specifically for its customers. The theory discussed within this document must be applied to custom libraries for Passfaces to work as described and to provide the appropriate level of security.
Passfaces is a patented technology and system. There are no other systems that use face recognition as a form of authentication available on the market.

New Users are Taken Through a Familiarization Process