

## **“An Application of Biometric Technology: Facial Recognition”**

### *Overview of Previous Article*

Our last article reviewed hand geometry recognition, primarily its key advantages; how hand geometry recognition works; and some of its popular, commercial applications.

This article focuses upon a biometric technology which certainly has gained its share of controversy: facial recognition, and is divided into the following sections: (1) How facial recognition technology works; (2) The application environments for facial recognition system applications; and (3) The various facial recognition technologies; (4) The privacy issues involved in deploying facial recognition applications.

### *How Facial Recognition Technology Works*

The science of facial recognition technology are generally the same as the other biometric technologies reviewed thus far in previous articles: (1) Acquisition of facial images; (2) Image processing of the facial images; (3) Unique feature extraction; and (4) Template creation. However, facial recognition technology can be limited by a different set of constraints when compared to other biometric systems. This is the case in the acquisition phase. For example, it is very crucial that the enrollment template is of very high quality for future identification and verification. Whereas other biometric technologies will allow for some margin of error (for example, as in the case of hand geometry recognition, a somewhat dirty hand can still be used to create an enrollment template), this is not true for facial recognition. The quality of the enrollment template is impacted by a number of factors. First, the user must look at the facial recognition camera at a close range and at certain angles so that a high quality enrollment template can be captured. The second factor is lighting. The lighting must be perfect in order to assure a good quality template. If the image is under exposed or over exposed in any way, this can have a negative impact on the quality of the template. Once these constraints in the acquisition phase can be overcome, the next phase is image processing. Here, the images of the face are converted into black and white images. These images are also cropped, rotated (clockwise or counterclockwise), and magnified. In the third phase, unique feature extraction, the facial recognition system looks for unique features around the sockets of the eye, cheeks, mouth, and nose. A constraint in this phase is that the structure of the face can change. For example, weight gain or loss can change the unique features of the face. Also, non biological changes in the face can have a negative impact upon unique feature extraction. This can include such things as wearing eyeglasses in the enrollment phase, but not wearing them in the verification phase, the removal of any facial hair, the wearing of cosmetics, etc. In the fourth phase, template creation, the enrollment template is composed from the unique features taken from the face. The enrollment template varies in size—from 100 bytes to 3 kilobytes.

### *The Application Environments for Facial Recognition System Applications*

Unlike the other biometric systems we have reviewed in previous articles (iris recognition, fingerprint recognition, and hand geometry recognition) implementing a facial recognition system can be much more complicated. For example, the other biometric systems can work in different kinds of application environments, and to a certain degree, are not impacted as much by the external variables which are present. This is not the case with facial recognition, as the performance of it can be greatly influenced by the type of application setting it is used for, and the external variables which are present.

The application environments for facial recognition systems can be further subdivided as “controlled” (verification) and “random” (identification). In a controlled environment, there is not much variation. The user will look normally into the camera, and good quality enrollment and verification templates will be produced. A typical example of a controlled environment is that of physical access entry at a particular location or site. However, in a random setting, there is a lot of variation. A typical example of a random setting is that of surveillance. Facial recognition systems have been used at airports for such purposes, and the results have been very mixed. This is because the facial recognition system has to identify and filter faces from different scenes which contain a lot of extraneous background noise (the “external variables”). The common belief is that the facial recognition system will be as good as the human brain in identifying individuals. However, reality dictates the opposite. The human brain has evolved over thousands of years. Facial recognition technology, although improving steadily, has a very long way to go before it reaches the sophistication of the human brain. Also, unlike finger scan and iris recognition where a positive match can be achieved, the facial recognition system will return a predetermined number of potential matches in a random environment. It is then up to the system administrator to determine the positive match.

### *The Various Facial Recognition Technologies*

There are various technologies that are employed in facial recognition systems to capture the unique features of the face. These technologies can be categorized as Eigenface; Neural Network; Automatic Face Processing; and Feature Analysis.

With Eigenface technology, the enrollment and verification templates are constructed via a database consisting of many 2-D, grayscale images of faces. So for example, if you were to be enrolled or verified by a facial recognition system, the image of your face would be reconstructed using the various 2D, grayscale images (the Eigenfaces). This reconstructed image would then serve as the appropriate template of your face.

With neural network technology, the system tries to “learn” which unique facial features will work best for verification and identification. Various algorithms have been developed and are utilized in order to accomplish this task. In order to help the system

“learn” which facial features will work best, different weight factors are assigned to the unique features found between the matched and unmatched templates.

Automatic Face Processing is an older technology. With this, the distances as well as the corresponding distance ratios are calculated between the unique features of the face.

Feature Analysis is the most commonly used technology. With this technology, the unique features are captured from the different parts of the face, as well as the relative position of these features. Also, this technology can take into consideration to a certain extent any changes in the appearance of the face.

### *The Privacy Issues Involved*

The use of facial recognition technologies aren't an invasion of privacy *per se*; however, as facial recognition technologies can be deployed passively in a random (identification) environment, the people they scan, extract features from, and attempt to identify may not even be aware of the process (let alone provide their consent). As a society, we don't fiercely object to the presence of a uniformed officer keeping a lookout for wanted criminals; at the same time, we haven't fully accepted the idea of a camera surrogate for such official presence.

So what are the differences between the officer and the camera? Nothing in principle. But cameras are cheap, and computers are very good at correlating data. So if facial recognition technology becomes accurate and fast enough, distributed surveillance of individuals is possible. (Facial recognition systems have a long way to go before anything like this could become practical.)

In controlled (verification) environments, privacy concerns are less an issue. The process of verification generally requires the active participation of a witting and consenting target, as is true for any biometric system. However, due to the limited accuracy of facial recognition technologies at present, especially *vis-a-vis* biological and non-biological changes in the face as described previously, you would have to remove various obstructions from your face. This means, then, that you can't successfully verify your identity while in disguise or while obscuring your face, should you need to authenticate yourself while remaining anonymous to human onlookers.

For others not involved directly in a biometric verification transaction, the privacy concern surrounding such a facial verification device mainly involve the presence of the camera. The use of biometric technology is irrelevant from the perspective of this privacy concern; there are cameras in public places already, and the same arguments regarding privacy apply to them as to facial verification cameras in public.

The next article will focus upon another biometric technology—speech/voice recognition.