Neil Lydick

A Brief Overview of Facial Recognition

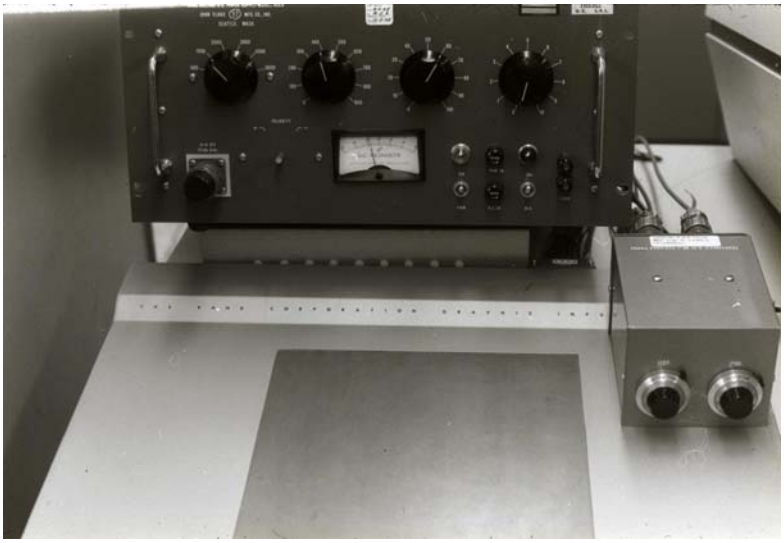
Introduction

Though we may take for granted our brain's ability to recognize the faces of friends, family, and acquaintances, it is actually an extraordinary gift. Designing an algorithm that can effectively scan through a series of digitized photographs or still video images of faces and detect all occurrences of a previously encountered face is a monumental task. This challenge and many others are the focus of a broad area of computer science research known as facial recognition. The discipline of facial recognition spans the subjects of graphics and artificial intelligence, and it has been the subject of decades of research and the product of significant government and corporate investment.

History

One of the pioneers of facial recognition, Woodrow Bledsoe, devised a technique called “man-machine facial recognition” in the 1960s. Bledsoe's technique, limited by contemporary computing and imaging technologies, involved classifying photographs of faces digitized by hand using a “RAND Tablet” (pictured on the following page) [4]. The RAND tablet was an electronic human input device consisting of a stylus that could be positioned at horizontal and vertical coordinates on a grid containing 1,000,000 distinct points on a 10-inch-by-10-inch tablet. The stylus' grid position was communicated via electromagnetic pulses [1]. In Bledsoe's method, an operator would utilize a RAND tablet to acquire the coordinate locations of various facial features. Among the facial features recorded by the system were the coordinate locations of the photographed individual's hairline, eyes, and nose. Records associating the name of the photographed individual with the numerical data recorded by the RAND tablet were then inserted into a database. Given a photograph of an unknown face, the system would use a method based on distances between facial features to retrieve the image in the database most closely associated with the provided photograph [4].

Bledsoe himself noted that there were many factors inhibiting a computer's ability to accurately recognize a single individual in two different photographs. Photographs of the same person might capture a person's face at vastly different angles, at different ages, with varying facial expressions, and under different lighting conditions [8]. Such minor changes in pose and environment could easily confound a computer algorithm that uses a distance-based approach to classify two faces as identical.



Photograph of a RAND Tablet, the progenitor of modern electronic stylus systems[1]

Modern Face Recognition

Since the 1960s, vast improvements in both algorithms and technology have greatly enhanced a computer's ability to perceive the same individual in multiple images. An example of a modern face recognition product is Identix' FaceIt, which boasts an intuitive user interface and conveniently automates much of the process. Some characteristics of the system bear a striking resemblance to the man-machine face recognition system devised by Bledsoe: the "landmarks" that FaceIt uses to classify faces include some of the same feature sets used in Bledsoe's design (e.g.: width of the nose, distance between the eyes); as in Bledsoe's system, these features are encoded and stored in a database [6].

FaceIt departs radically from systems of the past, however, in its use of a 3D model to describe the shape of the human face. Systems employing 3D face modeling can precisely store unique

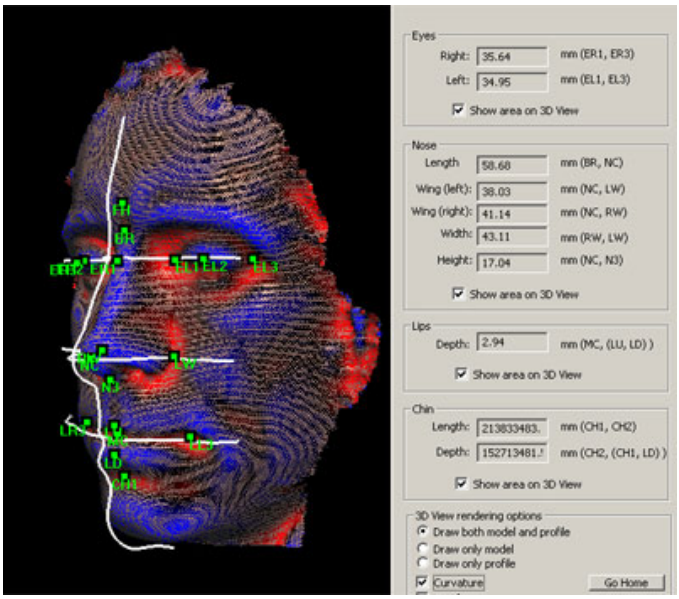
[1] Image credit: http://www.computer-history.info/Page4.dir/pages/PDP.1.dir/images/rand.tablet.jpg

attributes of the human face that do not vary significantly with age (e.g.: the curves of the eye socket, the contour of the chin) and are therefore more accurate than those that rely on conventional 2D face modeling [6]. Input to the system need not arrive through tedious RAND tablet manipulation. Instead, FaceIt uses data recorded by specialized cameras that provide it with the 3D data that it needs to generate a "faceprint," an encoded database entry. The program also supports input in the form of a scanned 2D photograph, but the system requires that a photographed individual be facing away from the camera at no more than a 55 degree angle to properly classify a 2D image (the requirements are less stringent for 3D images) [6].

One design challenge arises from the fact that a faceprint may be stored in either a 2D or a 3D format. When comparing a 3D database entry to a 2D entry to check for a match, the system transforms the data-rich 3D database entry into a 2D image using traditional viewing transformations. A proprietary algorithm then assesses the similarity of each image's facial attributes and outputs the correlation between the two images on a relative scale. The process is repeated on the set of images in the database, and the most relevant results are returned to the user [6].

Intriguingly, FaceIt's system can be combined with a supplementary product (also produced by Identix) that algorithmically analyzes the surface texture of a photographed individual's skin. Through a process called "surface texture analysis," the software mathematically models the skin and its pores as a 3D surface and stores the resulting data in the form of a "skinprint." If the user wishes to determine if an individual in a supplied input photo resembles an individual already pictured in the database, both the faceprints and skinprints are used to reject potential matches [6]. Though the company claims that the product, when used in conjunction with its traditional facial recognition software, increases accuracy by up to 25 percent, one must wonder whether the system could identify two photographs of the same individual taken at different ages or even during different seasons on the basis of skin (although the company does proclaim that skin recognition can differentiate two identical twins). Furthermore, it would seem almost impossible to derive minute details such as skin texture

from a conventional photograph. A successful application of the technology would almost certainly require images from a high resolution camera.



Screenshot of an image captured from an infrared camera in the facial recognition program Aurora, a FaceIt competitor[2]

Privacy Issues

While facial recognition is an imaginative and genuinely interesting field of study, many applications of facial recognition research have drawn the ire of privacy advocates all over the world. In its website advertising and downloadable brochure, Identix markets its facial recognition software to law enforcement agencies and casino gaming establishments. Some citizens resent a casino's ability to blacklist them and refuse them entry for virtually any reason. Others object to prolific use of cameras and identity tracking technologies by the government on the grounds that law enforcement should not be able to track people's movements and use such information to prosecute them without a warrant. Perhaps no country more aggressively monitors its citizens than the United Kingdom, which has installed roughly 1 CCTV camera for every 14 British citizens. Such cameras can be configured to identify individuals through face recognition [5].

Facial recognition is also an important component of the U.S. Congress' RealID initiative, a controversial program, which, among other provisions, would "require states to meet certain minimum

[2] Image credit: http://news.bbc.co.uk/2/shared/spl/hi/pop_ups/04/magazine_enl_1101314765/html/1.stm

security standards in order for the drivers' licenses and personal identification cards they issue to be accepted for federal purposes" [3]. If passed, the RealID legislation would require that driver's licenses carry a chip with a digitized photograph suitable for use in facial recognition databases maintained by law enforcement agencies [2]. Noted computer security expert Bruce Schneier argues that such well-standardized machine-readable data would promote identity theft and might entice bars or other businesses that regularly use driver's licenses while transacting business to sell consumer data to companies like ChoicePoint, which collect consumer data and credit information [7].

Works Referenced

[1] Davis, M.R. and T.O. Ellis. *Memorandum RM-4122-ARPA: The RAND Tablet: A Man-Machine Graphical Communication Device.* Aug. 1964. Rand Corporation. 10 March 2006 <http://www.rand.org/pubs/research_memoranda/2005/RM4122.pdf>.

[2] *Face Recognition.* 19 Jan. 2006. Electronic Privacy Information Center. 9 March 2006 <http://www.epic.org/privacy/facerecognition/>.

[3] Garcia, Michael J., et. al. *Immigration: Analysis of the Major Provisions of H.R. 418, the REAL ID Act of 2005*. 2 Feb. 2005. Electronic Frontier Foundation. 11 March 2006 <http://www.eff.org/Activism/realid/analysis.pdf>.

[4] Gates, Kelly. *Early Research on Machine Recognition of Faces.* Jun. 2004. University of Illinois at Urbana-Champaign. 9 March 2006 <http://www.acdis.uiuc.edu/research/OPs/Gates/contents/part2.html>.

[5] *How We Are Being Watched.* 3 Nov. 2006. British Broadcasting Corporation. 11 March 2006 <http://news.bbc.co.uk/1/hi/uk/6110866.stm>.

[6] Johnson, Ryan and Kevin Bonsor. *How Facial Recognition Systems Work*. How stuff works. 9 March 2006 <http://computer.howstuffworks.com/facial-recognition.htm>.

[7] Schneier, Bruce. *REAL ID.* 9 May. 2005. Schneier on Security. 9 March 2006 <http://www.schneier.com/blog/archives/2005/05/real_id.html>.

[8] *Facial recognition system.* 11 March. 2007. Wikipedia. <http://en.wikipedia.org/wiki/Facial_recognition_system>.