



FEMA

TechNote

U.S. Department of Homeland Security



System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. The SAVER Program conducts unbiased operational tests on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

Information provided by the SAVER Program will be shared nationally with the responder community providing life- and cost-saving assets to federal, state, and local responders.

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

For more information on this and other technologies, please see the SAVER website or contact the SAVER Program Support Office.

Telephone: 877-347-3371

Fax: 443-402-9489

E-mail: saver.odp@dhs.gov

Website: <https://saver.fema.gov>

Opinions or points of view expressed in this document are those of the authors and do not necessarily represent the view or official position of the U.S. Government.

This SAVER TechNote was prepared by the Space and Naval Warfare Systems Center, Charleston, for the SAVER Program.



Three-Dimensional Facial Recognition

Facial recognition is a biometric technology that measures unique facial characteristics to identify and verify an individual. The facial recognition process uses a computer to compare a new image with a previously stored image to determine if they match. Traditionally, law enforcement officers have relied on vision and memory to compare photographs to individuals in order to identify a suspect. Facial recognition technology enables officers to identify and verify an individual faster and more efficiently and also improves surveillance and access control capabilities.

The facial recognition field started with two-dimensional (2-D) systems. These systems operate successfully as long as the newly captured image is like the stored (enrolled) image—with similar pose, expression, lighting, and distance from the camera. If the captured image deviates in any of those areas, the chances of finding a direct match may be reduced.

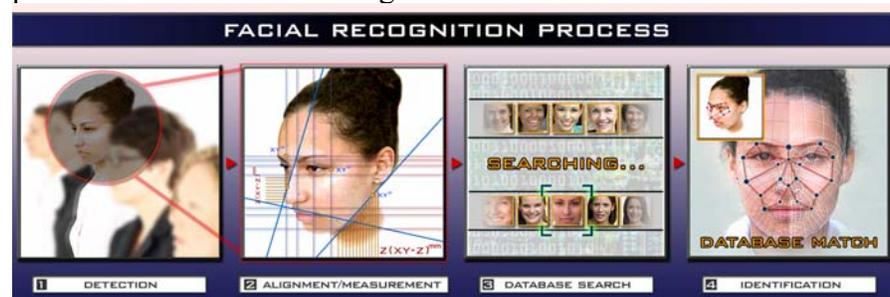
Three-dimensional (3-D) facial recognition uses the unique and variable structure of the face captured from multiple angles. Because the structure of a face is not affected by changes in lighting or pose, 3-D facial recognition offers the potential to improve accuracy over 2-D systems. As a result, 3-D technology allows for flexibility in image comparisons and greatly increases the probability of matching a subject to a photo from a database of images. Facial recognition with 2-D systems is more mature than 3-D systems, which are in their infancy. Development is continuing on both systems, improving them for the end user.

Technology Overview

Three-dimensional facial recognition is performed through the joint operation of computer hardware, software, and image capturing devices. The process of performing facial recognition includes:

- Capturing a facial image with a camera
- Processing the facial image with software to compare it against a database of enrolled images
- Identifying an image match

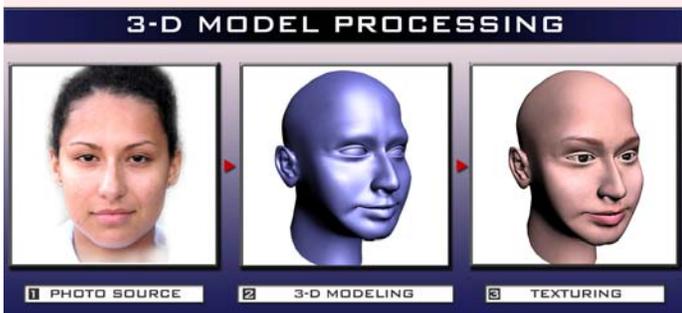
Behind the scenes, the software uses a series of complex algorithms that break down the facial structure into a format that mathematically compares the newly captured image to a stored photo. An example of this process is illustrated in the figure below.



The database of enrolled images can either be created by the organization or by referencing an existing database—such as mug shots, passports, or driver’s license records. The system will indicate if there is no match or if a match is found. In some instances, multiple matches may be found. When this happens, the recognition software will indicate to the user the probability of each match.

True 3-D facial recognition is accomplished when a 3-D enrolled image is matched to a newly captured 3-D image. This requires that a specialized 3-D camera be used to create both the enrolled and captured images to compare the 3-D geometry of a person’s facial structure. Since most database sources are currently 2-D, this limits the application of *true* 3-D facial recognition.

Three-dimensional facial recognition systems often refer to a mixed use of 2-D and 3-D technologies. Many facial recognition systems employ standard cameras, either digital or video, and apply 3-D algorithms to the captured image in order to create a new *virtual* 3-D image. A *virtual* 3-D image is developed by using a 2-D facial image and extracting key facial feature points, including points at the eyes, mouth, and nose, and synthesizing this information to create a 3-D model of the face. Some systems are capable of adding the additional dimension of skin texture to the model. The 3-D model process is illustrated in the figure below.



While *true* 3-D images are capable of increasing identification accuracy, many experts believe 3-D modeling is still a viable and practical method to accomplish 3-D recognition without having to incur the expense of specialized cameras in order to create a 3-D database.

Applications and Developments

Law enforcement has used 2-D facial recognition for access control, identification of subjects during investigations, surveillance, and booking and release processing of prisoners at detention centers. Three-dimensional facial recognition is applicable to these same applications, but provides greater flexibility for capturing an image depending on the products selected

and the algorithms used. No longer does the subject need to stand still directly in front of a camera waiting for their image to be captured. For some 3-D facial recognition systems, images can be extracted from video surveillance or crime scene video footage.

Systems are now under development that use 3-D technology to “fill in the blanks” of a partial image. For example, if an image is extracted from crime scene footage that reveals only part of a face, the software will create a model of the rest of the face. This model image would then be used to initiate the database search. This emerging capability may have the potential to offer the greatest value in the field of surveillance when applied to scanning large public gatherings, travel hubs, or domestic borders—all settings that may have obstructions or poorly lit areas, which can result in less than ideal images.

To further developments in the field, the National Institute of Standards and Technology (NIST) conducted the Face Recognition Vendor Test in 2006. The results of the vendor test indicated that human recognition abilities are not as good as some of the best performing algorithms.

Conclusion

Three-dimensional facial recognition systems continue to evolve and as 3-D systems mature they will provide new capabilities that 2-D systems may not be able to achieve. In addition, it is foreseeable that database sources of images will begin to shift from being completely 2-D to 3-D-based as the 3-D equipment matures and becomes more widely used. By working to overcome image capturing challenges, such as lighting and pose, scientists have developed the 3-D technology and equipment that provide:

- Greater flexibility in capturing an image
- More accurate images, generating a faster database match

Facial recognition technology will continue to be explored, expanded, and refined. New findings will likely lead to new ways to implement the technology for law enforcement.

Additional Information

NSTC Subcommittee on Biometrics
www.biometrics.gov

Face Recognition Vendor Test 2006
www.frvt.org/FRVT2006

Privacy & Biometrics – Building a Conceptual Foundation
www.biometrics.gov/docs/privacy.pdf