

CANDID

Computer-based Facial Recognition System Spots Terrorists Entering the U.S.

BY ELIZABETH O. COOPER

Carrying a fake passport, a would-be terrorist saunters through a major U.S. airport believing that he will be able to evade questions from immigration officers and freely enter the country.

What he does not see are the hidden cameras throughout the airport which are photographing him and following his every move. Nor does he realize that his facial image is rapidly being converted into a feature matrix with the resulting information sent by computers to embassies all over the world. Those embassies in turn will transmit any and all information about that person back to immigration officials at the U.S. airport. In short, his cover is about to be blown.

That scenario could soon play out in airports across the country thanks to groundbreaking research led by Old Dominion University's Vijayan K. Asari. The associate professor of electrical and computer engineering has spent the past three years developing a computer-based facial image detection and recognition system. The three-dimensional approach can detect, track and recognize faces in video streams, even those photographed in complex lighting and background conditions. Asari expects a prototype

to be ready for installation in the nation's international airports in the next two years, giving officials a new tool to identify potential terrorists trying to enter the United States.

64 Key Facial Details Generate A Feature Matrix

The facial image detection system is being developed through Old Dominion's Homeland Security Research Group, which Asari directs. Composed of engineering faculty and students developing projects in computer vision and image processing, speech recognition and networking, the group was formed shortly after 9/11 to find a universal solution for securing the homeland from intruders by developing a transparent environment. The group scored a major feat when the Department of Defense chose it as one of seven recipients to receive a \$68,000 grant to develop a system that would identify terrorists as they tried to enter the country. The defense department's initial call for research proposals resulted in 12,500 applications from all over the world. Other universities joining in the Old Dominion-led effort include Carnegie Mellon University and

CAMERA

Rensselaer Polytechnic Institute. The grant was recently renewed for \$300,000.

The face locating and tracking system would pinpoint all the detectable human faces in an image under varying background and lighting environments, camera positions, facial poses, size of the face regions and skin color. Asari realized that rapid and automatic recognition of faces from video sequences could be the key factor in identifying terrorists as they try to enter the United States via the nation's airports. However, automatic facial recognition is especially difficult because the number, location, size and orientation of human faces vary from frame to frame when taken by an ordinary video camera. Asari decided to develop a multidimensional feature matrix composed of key details about a person's face extracted from images captured by two surveillance cameras mounted side by side. One camera surveys the entire scene and detects faces in the image, while the other automatically zooms to the center of the detected face regions to capture more detailed information for additional analysis and feature extraction. The second camera's images are used to generate the face feature matrix, which is composed of 64 numbers. A similarity search between the resulting feature matrix and feature vectors stored in databases at embassies throughout the world should identify facial images on file that match those of the person under surveillance. Accordingly, the would-be terrorist is discovered.

“A person from an international flight must pass through INS checkpoints, but before he arrives at that point, we would have cameras to catch his face,” Asari explains. “We capture the image and derive from the face a feature matrix. That information goes into a computer connected to embassies around the world. By comparison, when we type a keyword into Google, all information relevant to that keyword pops up in the computer. Likewise, when that person's feature matrix is given as the keyword, it's going to search a connected server at embassies of cooperating countries. All information about that person will be available such as where he's traveled. If he's traveled to three countries, data from those three countries will pop up.”

Thanks to the high-speed computing system, the immigration services officer immediately receives details about the individual, including criminal history, and can question him based on that data or contact higher authorities for further investigation. “If no record comes up, he is not registered in any country,” Asari notes. “That's also bad because he must be in disguise because his face is not recognized by any country. He should also be investigated.”

Four different phases are involved in performing automatic facial recognition. The first is image enhancement, in which the surrounding environment is bright-

ened to reveal possible faces within the image and enable detection of skin color components. From there, human skin is identified and classified by color. Asari has made a universal human skin cluster and can match images with the cluster, thereby categorizing the individual by race.

The third stage involves discarding all non-facial regions, such as arms, hands and legs, from the skin regions that have been identified, so that only human faces are shown in the image. The face can then be matched with a database by analyzing facial features, such as the width of the nose, the distance between the eyes and the texture of the face. Asari says that there are approximately 250 facial images in Old Dominion's Very Large Scale Integration (VLSI) Systems Laboratory, but that number reaches into the thousands when the U.S. government's database is included.

Fourth Stage: Tracking

Following the successful completion of image enhancement, skin identification and facial classification, the tracking stage comes into play. “We need to track the face because we don't want him to disappear,” Asari notes. “If he moves away, we can communicate that information to other systems. If cameras are fixed at every 100 feet in an airport, they can communicate with other cameras. It's a transparent environment.”

He adds that individuals will not realize that a camera is trained on them because the equipment is very tiny. Also, the images themselves are not transmitted. “The moment the camera catches the image, we are converting the image into a face feature matrix. From that matrix, we never see the original image,” he says. “Only the camera is watching you, and it immediately converts that image to a set of numbers which represent the facial features of a particular person.”

Those numbers are generated by an algorithm based on spatial locations of facial features and depth information of those features. Asari notes that 64 numbers come from various aspects of an individual's face. “Everybody's face is different, so 6 billion people in the world have 6 billion kinds of feature matrices. There would definitely be different combinations for different people.”

It takes 125 milliseconds to perform the search of feature matrices. “We can have eight frames in one second,” Asari notes. “It's immediate. We can also have multiple images of the same scene at the same time.”

Using Los Angeles International Airport as an example, images photographed from the first camera are converted into a facial feature matrix and transmitted by a router to the main airport computer. From there, the matrix would be sent to the main computer for the western United States, which is connected to servers at all airports in that region, as well as to international air-

ports and embassies. "Within seconds, we would get all the data we need," Asari says.

In addition to the grants, the defense department is supporting the project through connections to servers at embassies around the world. The department is also working with various industries to develop cameras and a computer network to test Asari's prototype.

Security is a major concern in developing the facial recognition system. The image analysis and feature extraction is performed using computer hardware designed by engineers in the VLSI Systems Laboratory, with the matrices encrypted and protected from corruption through a virtual private network. "Nobody is able to intrude in a feature matrix and corrupt our data," Asari says.


The specially designed computer hardware ensures that the system will work faster and be more reliable. "We don't want general computers because general computers do several other jobs. This hardware does this job alone. If we make an application-specific system, it does a specific job with maximum efficiency and speed."

Speed is the biggest factor in designing hardware, says Asari, noting that general computers can only perform programs sequentially. "With this hardware, the job is done in one shot. You get the output in a fraction of a millisecond."

Applications Beyond Ports of Entry

Although the system's main objective is recognizing potential terrorists as they travel through international airports, Asari says it could also be connected to servers at courts and police stations across the nation. Such a device would allow officials to search records of everyone convicted within the United States. "A camera at a shopping center could incorporate the system to get data for security officers to keep an eye on a person," he adds. "That's a lower application of the same concept."

Individuals could also one day employ the facial detection system in their homes. "We can do a search of people coming to the door by creating a face feature matrix," Asari explains. "If I keep a camera at the front entrance of the house, it catches an image of a person coming to the door. Security centers have a database of criminals, and the security system keeps track of people coming to the door. The moment the camera catches his face, details are created and come up on the computer at the security center. The security center places a call to the house to warn the people inside the house not to open the door because that person is a convicted criminal somewhere."



"Everybody's face is different, so 6 billion people in the world have 6 billion kinds of feature matrices. There would definitely be different combinations for different people."

—Vijayan K. Asari