FBI

Print | Email | Contact

Facial Recognition Programs Revolutionize FBI's Use of Images

By Amy K. Hotz, OPA, video produced by Alexander Scaltrito

Closed captioned version
Voice over by Tracy K. Simpson, OPA

(U/FOUO)

In 2009, case agents in Florida closed in on a suspect. They knew this person was in a theme park--and that presented a problem. It was impossible to physically surveil him through crowds of innocent bystanders casually enjoying their vacations.

But, like many public places today, lines of sight from multiple security cameras crisscrossed the area.

Obtaining the footage was relatively easy. But how would they trace this person in hours of images from each camera as he moved from one area to another?

Investigators contacted Senior Photographic Technologist Richard Vorder Bruegge, Ph.D., of the Operational Technology Division's Forensic Audio, Video and Image Analysis Unit (FAVIAU) in Quantico. They told him they need software that can find and identify a person who intermittently appears in hours of videos.

"At that time, we couldn't do that yet. I said, 'Call back in a year or so,' " Vorder Bruegge said.

A year makes all the difference. Vorder Bruegge brought the request to the attention of the unit and in August 2010, the Mitre Corporation with the help of PittPatt (Pittsburgh Pattern Recognition) delivered two new facial recognition programs to Quantico. Vorder Bruegge and others expect the programs to

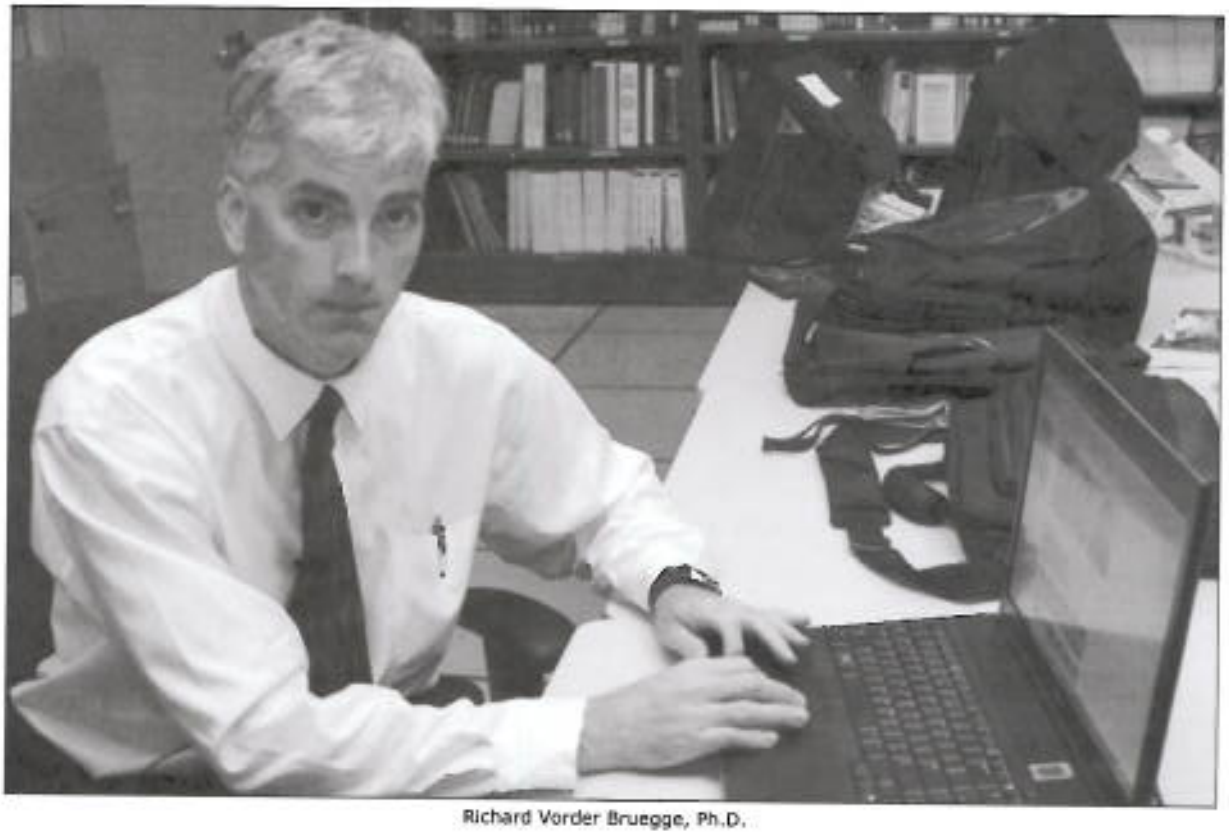
revolutionize the way the FBI uses still and video images.

With AFDAR-V, or Automatic Face Detection and Recognition for Video, an investigator can input hundreds of hours of video--even poor quality footage--and ask the program to find all the faces. AFDAR-V will then group those faces to show the user each video segment in which each person appears, and it will mark those segments on a timeline for easy navigation.

Its sister program, AFDAR-C, clusters still image photographs. If an investigator has a database of photos, mugshots from police stations or passport photos, for example, AFDAR-C will group together the images of persons who appear more than once in the database. If the investigator has a photo of a known subject, that picture can be uploaded to see if other photos of that person exist in the database.

In each case, it's up to a trained human analyst at the Criminal Justice Information Services Division (CJIS) to double check that the software's results are correct. Regardless, what would have taken a team of people days or months to analyze is cut down to hours or even minutes.

"You need human beings to be judicators on that. And so some of the people that used to do fingerprint searching at CJIS are going to be doing face searching for us," said Vorder Bruegge.



Richard Vorder Bruegge, Ph.D.

This technology is so new in the FBI, there hasn't yet been an opportunity to use AFDAR-V in a real case. But just a few months ago AFDAR-C proved its worth in a case that overwhelmed agents and analysts.

"It was like a dream come true. It really was," said SA Theresa Fanelli of the Newark Field Office. "In order to charge someone with aggravated identity theft, you have to have the IDs they obtained. So if we didn't have those beforehand, without the help of Richard, I don't know that we would've been able to charge them. I guess we could've tried to go back and piece it together afterwards and gone back and charged them, but you know how that goes after the cat's out of the bag."

SA Fanelli and a team that included Barbara Woodruff, Mark Bendul, Nathan Kim, Moon Kim and Christina Lee worked on "Operation Golden Brokers," a spinoff of "Operation Paper Mountain," a complicated case that opened in Chicago in 2009.

Agents there had noticed a spike in the number of people applying for Illinois driver's licenses with 586 social security card prefixes. From 1970 until 2002, only about 500 people in that state held 586 prefixes. But from 2003 until 2005, the number climbed into the thousands.

Through years of investigating, SA Dave Patch of the Chicago Field Office was able to piece the story together: Chinese nationals traveled to U.S. territories including Saipan, American Samoa and Guam to work in American factories. This entitled them to a U.S. social security number starting with 586.

When their job ended, the cards were either sold or stolen and sent to clearing houses in the United States. Illegal brokers would then buy the cards from the clearing houses and set up offices in areas with large Asian populations.

Recent immigrants would go to these brokers and buy identity packages for about $3,500 which included a social security card of someone with a similar age. Fake passports were created using the person's actual photo but fake social security number. With these documents, the broker would actually escort the customer to a DMV office to register for a legitimate driver's license.

For an additional fee, the broker would spend a couple of months building up the customer's credit score. The customer would then go to stores, buy cars and max out credit cards but never pay any of it back.

"It was limitless, the amount of fraud they were engaged in – to include filing for false tax refunds with the IRS. There was nothing off limits," said SA Fanelli. "They weren't looking for any legitimate ID because they were having problems with immigration or anything like that. They were simply looking to steal money . . . . It was really lucrative. The business was so blatant that brokers would advertise in the newspaper and say, 'We can help if you need a 586.' It was bad."

The second installment in this two-part series will illustrate how AFDAR-C was instrumental in solving a complicated fraud scheme involving thousands of new Asian immigrants.

(U/FOUO)