Taking a Byte out of Crime

Police hail computer system that cracked the Night Stalker case

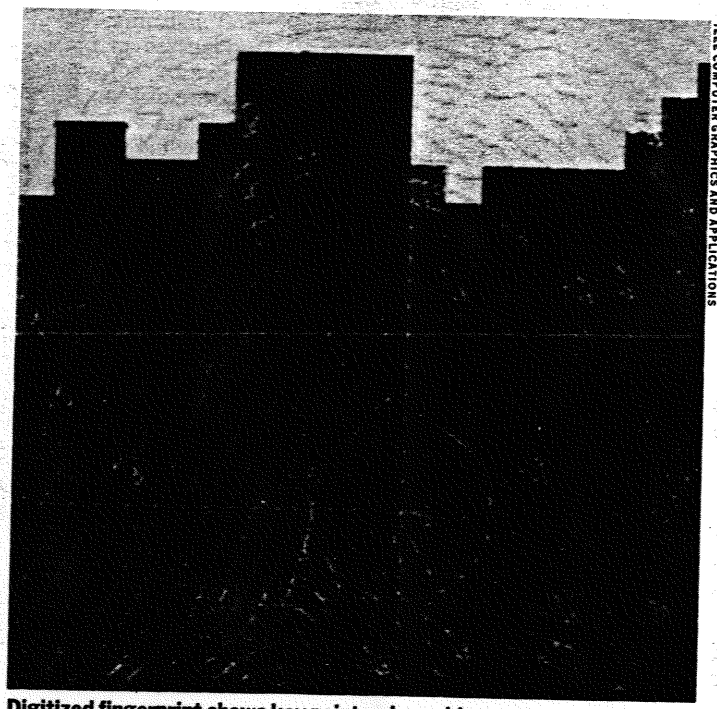
Three minutes after California's new automated fingerprint identification system received its first assignment, the crime-stopping computer scored a direct hit. It matched a smudged print lifted from an orange Toyota in Los Angeles to one taken from a 25-year-old drifter with a record of drug and auto-theft arrests. Two days later, Richard Ramirez was caught and charged with one of 15 murders attributed to the Night Stalker, the serial killer who had been terrorizing the city for the past seven months.

The speedy identification of Ramirez was the latest and most dramatic example of a technique that has police officials across the U.S. clamoring for fingerprint identification computers of their own. Says Brooklyn District Attorney Elizabeth Holtzman: "It could revolutionize law enforcement in a way that no other technology has since radios were put in patrol cars."

Fingerprint identification of criminals has been routine since the turn of the century, when Scotland Yard pioneered its systematic use. Computers were brought into the process in 1976, when the FBI began converting some 17 million prints to digital form. Today, every armchair detective knows better than to pick up a gun by its handle, lest he obliterate fingerprints that could identify the killer.

But real policemen know that they rarely get good prints from a handgun and that any they do find are often useless. Fingerprints can prove that a particular suspect was at the scene of a crime, but when investigators have only prints and no suspect, the odds of finding a match are greatly reduced. Los Angeles police estimate that it would have taken a single expert searching manually through the city's 1.7 million print cards 67 years to come up with Richard Ramirez's prints. "Frankly speaking," says Commander Bill Rathburn, "most of the dusting for prints we do is for public relations purposes, to show people that we're doing something to pursue the criminal."

The problem is that it takes too long to pick out the intricate patterns of ridges that distinguish one person's fingertips from the millions on file. Before computers, these patterns were classified into eight categories of arches, loops and whorls. To speed up the search, the FBI's system concentrates on simpler patterns: the so-called points of minutiae, where a ridge line ends or a single ridge splits into two. A thin beam of light scans each print and records the location of up to 100 minutiae. The computer then converts these data into numbers that can be stored on magnetic disks and retrieved for comparison with prints taken from the scene of a crime.



IEEE COMPUTER GRAPHICS AND APPLICATIONS

Digitized fingerprint shows key points where ridges stop or split in two

DOUG PIZAC—A.P.

Richard Ramirez

This method has scored some dazzling successes over the years. The Royal Canadian Mounted Police, for example, used it to trace prints from a box of pizza to a professional hit man who had gunned down a target while posing as a delivery boy. But some police complain that their computers are too slow and too undependable for routine police work. A typical computer search of the files can take more than six seconds per fingerprint and often overlooks prints that are even slightly smudged.

The computer that cracked the Night Stalker case was designed by the Nippon Electric Co. to overcome these deficiencies. It combines high-speed, custom-made silicon chips with a new technique for analyzing points of minutiae. Besides plotting each point, the computer also counts the number of ridge lines between that point and its four nearest neighbors. This provides a fairly good measure of the relative position of minutiae points; if two minutiae taken from a print in the police files are separated by eight ridge lines, chances are they will be separated by the same number of lines in a print that has been distorted or blurred. The system's designers were certain that this extra measure would result in dramatic improvements in performance.

They were right. The city of San Francisco started using a NEC fingerprint system in 1984 and almost immediately began picking up prints that previous searches had missed. Flipping through 650 prints a second, the new computer took only seven minutes to identify a man who had fatally shot a 47-year-old woman during a 1978 robbery attempt. In its first four days of operation, the system cracked 34 unsolved cases. News of the computer's remarkable performance traveled quickly. One month later, NEC sold a second system to the state of Alaska, and eight months after that, California decided to scrap its existing system in favor of one built by NEC.

In the Night Stalker case, technicians in Sacramento were still loading records from the old system into the new when the suspect print was lifted from an automobile linked to the killer. At the urgent request of police, four NEC programmers worked all night to finish the job. The following day, after the fingerprint had been scanned and digitized, the computer compared it with 380,000 stored in its memory and spit out the names of the ten people whose prints most closely resembled it. At the top of the list, with a probability rating four times as high as that of the nearest contender, was Ramirez. Says Elton Johnson, NEC's West Coast manager: "We knew immediately that we had our man."

Los Angeles police, eyeing their roster of unsolved crimes—4,350 murders, 2,500 rapes, 4,000 robberies and 20,000 burglaries—cannot wait to plug these cases into the state's new system. Other California lawmen share their enthusiasm. "There are a lot of people walking the streets out there who think they're home free," says Orange County Lieut. Richard Olson. "Once we get these computer systems working together, they're going to be in for a surprise." ***—By Philip Elmer-DeWitt. Reported by Anne Constable/Washington and Dan Goodgame/Los Angeles***