

EVIDENCE

TECHNOLOGY MAGAZINE

The magazine dedicated exclusively to the technology of evidence collection, processing, and preservation
Volume 11, Number 5 • September-October 2013



Fingerprint Powder

TOPICS IN THIS ISSUE

- The Independent Crime Lab Concept
 - DNA Lab Design
- Surveillance Video with DSLRs
 - Facial Recognition



FACIAL RECOGNITION: *The most "Natural" Forensic Technology*

PEOPLE WATCHING has been around for as long as—well, as long as humans have lived on earth. While usually dismissed as just a way to pass time, many will tell you there is an art to watching people. First of all, people-watching is something that is done in a latent way. That is, it is done in real time without the knowledge of those being watched. And many are quick to say this does have redeeming, practical uses. Many authors have used people watching as inspiration for characters in their books and stories. Authors claim seeing people on the street or in a restaurant and eavesdropping on what they are saying can be extremely informative and inspirational for a person who is trying to create a new story.

But of all these body-language signals or verbal clues, it is the human face that is most telling: A face remains the most widely used way of identifying or authenticating a person. A photo of it is on most of the identification documents that we carry in our purses and wallets. A lot of information can be provided from a person's face, clothing, and appearance, and today a person's face has become the epicenter of the most fascinating and promising evolving forensic technology: facial recognition software.

While humans have always had

Written by John Dowden

the innate ability to recognize and distinguish between faces, computers only recently gained the same ability. The history of developing facial recognition software started in the mid-1960s, when scientists began working on using computers to recognize human faces. Since then, facial recognition software has progressed significantly.

The first semi-automated facial recognition programs required locating features—such as the eyes, ears, nose, and mouth—on a photograph. Then, distance and ratios to a common reference point were determined and compared to reference data. This process evolved into using a range of specific body indicators such as hair color and lip thickness, and recognition of these characteristics was automated. Still, measurements and locations needed to be manually computed, requiring a significant amount of labor during the process.

By around 1990, mathematical formulas were being applied to the process. This development was significant because, for the first time, a finite number of values could be aligned to code and identify a face. This process was called "eigenfaces," which used a small vector square area

(eigenvector) of a face to apply measurements and identifiers. Remarkably, it does not take many eigenfaces combined together to achieve a fair approximation of most faces. This technique of creating eigenfaces and using them for recognition also found use outside of facial recognition, in applications such as handwriting analysis, lip reading, voice recognition, and sign language or hand-gesture interpretation.

The science of facial recognition was surging forward and improving accurate identification through technology. This step-by-step process or algorithmic application continued to progress and propelled facial recognition from its infancy to a market of commercial products. With algorithms now inherent in the facial recognition process, the technology could be evaluated for accuracy. Standards were established and vendors of facial recognition software could then be measured for accuracy and application.

Incremental technology advances used a 2D image to compare or identify another 2D image from a database. To be effective and accurate, the image captured needed to be of a face that was looking almost directly at the camera, with little variance of light or facial expression from the image in the database. Of course, database images are rarely taken in a

controlled environment. Even the smallest changes in light or orientation can reduce the effectiveness of a system, rejecting a match to any face in the database, and leading to a high rate of failure.

Current facial recognition software now uses a 3D model and captures images in real time to select distinctive features of the face—where rigid tissue and bone are most apparent, such as the curves of the eye socket, nose and chin—to identify the subject. These areas are all unique and don't change over time. 3D facial recognition can even be used in darkness and has the ability to recognize a subject at different view angles, potentially up to 90 degrees (i.e. a face in profile).

Better and less expensive (and increasingly ubiquitous) cameras are addressing challenges and issues associated with grainy and blurry images. While current international standards require a resolution of 90 pixels between the eyes for facial recognition algorithms, some are producing results well below this threshold. Static image databases remain a key part of identifying and tracking a face, although video streams can be much more useful.

And even when facial recognition technologies improve and mature, the question still remains: is facial recognition ready for prime time and will it gain everyday acceptance? The answer right now is, "It depends." In recent tests, some systems that compare live people to their passport photos at airports still have an overall error rate of about 15 percent. If performance in such controlled situations has such variation, it would seem there is still a lot of work to do before these systems can automatically, and accurately, pick out faces of interest from surveillance footage. But that is not an accurate depiction of the technology's future because advances are being made at an extraordinary rate.

How it Works

Once it detects a face, a facial recognition system determines the head's position, size, pose, and unique characteristics.

Every face has numerous, distinguishable landmarks—the different

Is our most distinguishing human feature a panacea that will make our world safer?

peaks and valleys that make up facial features. These landmarks are called nodal points. Each human face has approximately 80 nodal points. Some of the nodal points measured by the software include:

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

The system translates nodal-point measurements into a numerical code or set of numbers, called a faceprint, representing the features on a subject's face that can be compared to faces in the database. A match is verified from the faceprint.

Real Case Scenarios

The most recent high-profile case involving technology to identify suspects is the Boston Marathon bombing in April 2013. Opinions are mixed on whether facial recognition technology was used or helped in the search for the Boston bombers, but one thing is clear: video surveillance *was* very useful in tracking the movements of the suspects. The images released of the Boston suspects had 12 to 20 pixels while high matching requires around 90 pixels.

The Pennsylvania State Police with PaJNET system has used facial recognition within their statewide mugshot system to solve many real crimes. This system is used by hundreds of local and state law enforcement within Pennsylvania, but also by the U.S. government to solve crimes:

- United States Marshals Service—Searching for an Individual Wanted for Several Offences: *The United States Marshals Service (USMS) contacted Pennsylvania*

There are many reasons why facial recognition technology is becoming more accepted, prevalent, and accurate:

- 1) Facial recognition is far easier technology to implement, operate, and support in practical use.
- 2) End users need not be biometrics experts in order to perform and review facial recognition searches.
- 3) Explosion of camera-enabled phones and tablets has led to capturing millions of photographs and videos.
- 4) Faces can be identified and taken easily by regular users with minimal training to verify the face-matching results.
- 5) The face-capturing process is non-intrusive, contactless, and less restrictive. Images of faces can readily be taken from a distance (50 feet or less) for facial-recognition purposes depending on the resolution of the camera. Live cameras can even be installed in remote places of an area, campus, or facility.
- 6) Continued investment in enhancement of the technology by biometric companies such as NEC.

FACIAL RECOGNITION

Criminal Intelligence Center (PaCIC) for fugitive location assistance. PaCIC used facial recognition technology to search drivers' licenses, leading to a match against an alias. PaCIC then queried other databases leading to apprehension of the fugitive by USMS.

❑ United States Secret Service—Investigating \$300,000 loss from Identify Thefts: *United States Secret Service (USSS) and local law enforcement spent more than six months in vain using traditional investigation techniques. Surveillance photos were uploaded into the mugshot and facial recognition system for a search. A match was made within two hours. USSS made the arrest and filed charges against the ID theft ring.*

A recent study conducted by Michigan State University (MSU) simulated the post-forensic activity of the April 2013 Boston Marathon bombings. The study examined the reliability of automated facial recognition (AFR) software in assisting law enforcement in identifying bombing suspects. In the MSU simulation, researchers used actual law enforcement video from the bombings and searched the footage against a background database of 1 million law enforcement booking images. They

In a Michigan State University simulation, researchers used actual law enforcement video from the Boston Marathon bombings and searched the footage against a background database of 1 million booking images. They registered a match with suspect number two.

found that the NEC NeoFace product registered a “rank one” identification—a match—of suspect number two. The study also found that the NEC NeoFace solution consistently registered highly accurate facial matching scores in the study’s simulation.

Note: The MSU technical paper on evaluating automatic facial recognition technology can be accessed at: www.cse.msu.edu/rgroups/biometrics/

Application of the Technology
Field forensic work is a natural application for facial recognition. Field agents equipped with PDAs can submit

search requests to remote facial recognition systems or even a watch list on the device itself and quickly determine whether an individual is already a known felon.

In the near future, other applications for using facial recognition could be applied. For example, agencies in airports could use variations of facial recognition to screen foreign travelers. Fingerprints and photographs will be checked against a database of known criminals and suspected terrorists. When the traveler arrives in the United States at the port of entry, those same fingerprints and photographs will be used to match the person’s visa as being the same person attempting to gain entry.

While the primary users of facial recognition software typically have been law enforcement agencies, more potential situations in which the software could be used are becoming possible. Other potential applications include ATM check-cashing security and employee access control as well as time and attendance, customer loyalty, and VIP screening. The software is able to quickly verify a customer’s face. After a customer consents, a digital image of him is captured. This then generates a faceprint of the photograph to protect customers against identity theft and fraudulent transactions. It is likely that using facial

AUREUS 3D
IDENTITY ACCELERATOR



Aureus 3D® Identity Accelerator is the only tool available to create actionable mugshots out of video images. Instantly turn any user into a 3D imaging pro! The results are so remarkable, you need to see this for yourself.

Contact us today for a free evaluation copy!

- ✓ Easy to setup and east to operate
- ✓ Add multiple images to build a better 3D model
- ✓ Input images or videos - or both!
- ✓ Automatic face finding
- ✓ Automatic pose correction
- ✓ Works with all face recognition software

CyberExtruder
211 Warren Street
Newark, NJ 07103
T 973-623-7900
www.cyberextruder.com

imprimusSM

Imprimus Forensic Services, LLC

**Training for the
Crime Scene Professional**

**Crime Scene Investigator's School
Footwear & Tire Track Evidence
Photography & More**

*We feature programs held in conjunction with the
Northeastern Illinois Public Safety Training Academy.
Visit our website for more information.*

P.O. Box 1532
Arlington Heights, IL 60006
847.804.8420

www.imprimus.net

FACIAL RECOGNITION

recognition software will eliminate the need for a picture ID, bankcard, or personal identification number (PIN) to verify a customer's identity and greatly prevent fraud.

Looking Ahead

"Facial recognition remains a major focus of forensic research because of its non-invasive nature and because it is people's primary method of person identification. It has enormous promise in both law enforcement and commercial applications," said Raffie Beroukhim, vice president of the NEC Biometrics Solutions Division.

Despite some skepticism, today's algorithms are more than ten times more accurate than the facial-recognition algorithms of a decade ago and 100 times more accurate than those of 1995. Algorithms now outperform human perception in recognizing faces and can even identify identical twins. The market continues to gain acceptance, growing at about 60 percent annually and is expected to exceed 1 billion in 2013. Facial

Today's algorithms are more than ten times more accurate than the facial-recognition algorithms of a decade ago and 100 times more accurate than those of 1995.

recognition as a biometric technology is a powerful tool for law enforcement to improve public safety by assisting with crime-solving: "If we catch one murderer that would otherwise have gotten away, this solution has paid for itself," said Harry

Giordano, manager of special projects with the Pennsylvania Justice Network.

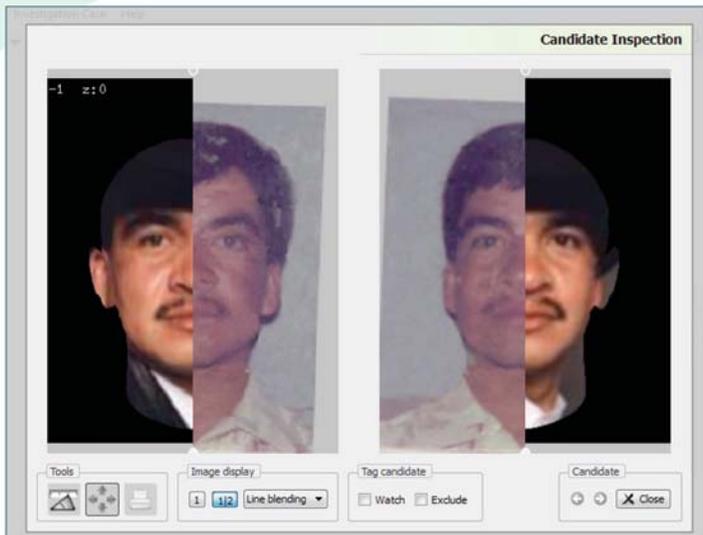
Facial recognition is a technology that is becoming more commonplace, more accepted, and most importantly, indispensable. Concerns about civil liberties and privacy will play out. And, because of its potential to make life better and safer, many forensic experts foresee facial recognition technology becoming part of society's fabric. ☺

About the Author

John Dowden is the Senior Product Manager for NEC Corporation of America Biometrics Solutions Division. He has over 16 years of industry experience planning, developing and implementing multi-modal biometrics products and solutions for implementation and operation across the world. Before working in biometrics, he was both a military officer with the Air Force and electrical engineer within private industry.

john.dowden@necam.com

Market-leading face recognition technology



for fast and accurate criminal investigation

FaceVACS-DBScan with Examiner instantly matches crime scene photos, composites and surveillance video images against your mug shot repository to support efficient suspect identification.

The Examiner toolset enhances probe images to achieve faster and more accurate match results.

www.cognitec.com

Cognitec develops market-leading face recognition technologies and applications for enterprise and government customers around the world. In various independent evaluation tests, our FaceVACS® recognition software has proven to be the premier technology available on the market.

