Iris-Scan Authentication Cuts Fraud in Connecticut Vehicle Emissions Testing

BY: Thomas J. Fournier | June 17, 2005

With the help of increasingly sophisticated digital imaging techniques, advanced software processing algorithms and faster computing speeds, the measurement of human biometrics has become a practical tool applicable to everyday system user authentication. This article examines one such application where user authentication via iris scan has successfully migrated out of the clean and controlled office environment into the less friendly realm of automotive repair shops. An iris-scanning application provides the Connecticut Department of Motor Vehicles with certainty and traceability regarding the identity of some 1,300 licensed inspectors performing government-mandated emissions tests in hundreds of private enterprises throughout the state.

In the post-911 environment of increased emphasis on security, biometric authentication of system users has received considerable focus as more business and government agencies seek to overcome the shortcomings of badge-and-pass code identification. Those shortcomings include high administrative costs as well as reduced certainty of authentication due to pass code and card sharing or theft.

Biometrics is synonymous with "biometry," the statistical study of biological phenomena. In our case biometrics more specifically refers to measuring unique physical characteristics for verification of personal identity. A number of biometric measurement techniques have been developed and are commercially available, including analysis and characterization of the human iris, fingerprints, hand, voice, face and even vein patterns.

In March of 2001 the National Physical Laboratory (NPL) in Middlesex, U.K. -- the UK's national standards laboratory -- published a study evaluating the efficacy of all six of these biometric authentication methods.(1)

The biometric study was conducted by NPL's Centre for Mathematics and Scientific Computing and it rigorously evaluated various biometric authentication devices using 200 volunteer subjects. NPL found that, when compared to the other five biometric identification methods, the iris-scanning method was the most accurate. Test subjects were "enrolled" onto the iris scan system by sitting before a small, special purpose digital camera and waiting a few seconds for the associated computer and software to characterize and memorize the unique patterns within the detail of one of their irises. From there the subject was invited back for multiple attempts at iris identification over a period averaging 55 days. The procedure on the follow up visits involved seeing whether the iris-scan system would accept or reject the subject's claimed identity based on comparing the current iris scan with the iris scan stored during enrollment. It also involved seeing if the system would accept them under a falsely claimed identity.

An inspector logs in. The iris scanner is the small tilted object on the table, below and to the left of the Vehicle Identification Number bar-code scanner. The inspector's eye appears on the top left of the monitor.

NPL found that the iris scan system had an impressive zero false acceptance rate, meaning that it never accepted a person claiming a false identity. Its false rejection rate -- meaning the frequency with which it denied access unfairly -- was only 1.8 percent for single tries and less than 0.2 percent when a legitimately enrolled subject tried as many as three times to get system access. All of the other biometric methods had false acceptance rates dramatically higher.

In general, where the sensitivity of a biometric measurement system is adjustable, there is a trade off between false rejection rates (legitimate user denied access) and false acceptance rate (illegitimate user allowed access). As the machine is adjusted to reduce the probability of letting an illegitimate user gain access, the number of legitimate users denied access tends to go up. For example, according to the NPL study, when the various systems tested operate so as to achieve a false acceptance rate of 0.01 percent (1 in 10,000 illegitimates gain access) the percentage of legitimate users that would be denied access is shown in the table below.

Table 1 -- False Rejection Rate

Percentages are rounded approximations. Iris data shown for 0% False Acceptance Rate, all others for 0.01%

Iris scanning: 2 percent reject after one try; 0.2 after three tries
Fingerprint: 6 percent reject after one try, 2 percent after three tries
Voice: 11 percent reject after one try; 4 percent after three tries
Hand: 26 percent reject after one try; 9 percent after three tries
Face: 44 percent reject after one try; 41 percent after three tries
Vein: 44 percent reject after one try; 38 percent after three tries

---

As can be seen from the table, when the various biometric systems are adjusted to provide a high level of certainty that illegitimate users will be denied access, the iris-scan method is the least likely to turn away legitimate users.

So what is it about the human iris that makes it so useful for identification purposes? The iris is the colored ring of the eye encircling the pupil. Like fingerprints, no two irises are alike. According to Dr. J. Daugman(2), a research scientist and renowned developer of iris identification techniques, a given human iris has so much statistical variability that the chance of any two matching is about one in 7 billion. Genetic twins possessing the same DNA have completely different irises and, in fact, even your own left iris is different than your right iris.

Iridian Technologies, the manufacturer of a leading patented iris authentication system, explains why this statistical variability occurs in a tutorial appendix to their operation guide(3). They state that the iris pattern development process begins in the womb about six months after conception and, once complete, the pattern remains stable for life. Each iris is unique because a completely random process in the womb forms it. Close examination of your own iris will reveal a variety of small-scale features that scientists have categorized and given names such as: crypts, radial furrows, pigment frill and collarette. Iridian's iris authentication system works by dividing the iris video image into concentric rings call demarcation zones and digitizing the small-scale features of each zone. The result is a unique binary iris code that is stored during enrollment of the user on the system and later used to compare when the user comes back to gain access.

It all sounds impressive in theory, but does it work in the real world?

Connecticut DMV

In October of 2003 Applus+ Technologies, Inc. pioneered the first ever application of an iris scanning authentication system in a vehicle emissions inspection program. The Applus+ application is groundbreaking because they use the iris authentication system in the rough and dirty environments of hundreds of private automotive repair shops. Under contract to Connecticut's Department of Motor Vehicles (DMV), Applus+ provides the iris scan system to 270 independent inspection and repair facilities to authenticate some 1300 licensed inspectors before each and every government-mandated vehicle inspection. Approximately 900,000 vehicles are inspected via that system each year. Applus+ provided each of the private inspection stations a complete set of computerized emissions analysis equipment, including the integral iris authentication camera and its associated software.

"Representatives from the DMV initially enroll the inspectors by checking valid identification and having the iris scanner memorize their iris," said Jim Valerio, the Connecticut Program Manager for Applus+ Technologies. "From then on the inspectors must use the iris scan so that the emissions measurement system can authenticate their presence prior to conducting an official vehicle inspection."

Authentication is simple. The system user merely looks into the iris-scan camera from a distance of about 20 inches and within a couple of seconds the authentication is complete. Even in the rough and dirty environment of the automotive test and repair shop, Applus+ Technologies has found that 98 percent of the time the iris scanner is able to identify a previously enrolled inspector, thereby allowing him or her to proceed with the official vehicle inspection. In those relatively rare instances where the system is unable to

identify an enrolled user, a backup system of card and pass code is allowed so that motorists are not inconvenienced waiting for the inspector to resolve the problem. In such cases, however, the system automatically tracks the authentication procedure variance and Applus+ personnel viewing the variance data remotely will contact the inspector to resolve the authentication issue.

The Connecticut DMV performs its own internal audit of the authentication procedures and they give the iris-scan technology high marks. Tim Kulish, the Division Manager for Connecticut DMV's Emissions Division reports that, "This technology and our internal audit procedures have virtually eliminated authentication violations that were commonplace with the badge-and-pass code verification system."

The particular iris scan system chosen by Applus+ Technologies for the Connecticut vehicle inspection program operates in conjunction with an ordinary Pentium PC computer and is based on a special purpose video camera operating under ordinary room lighting conditions. This means that no lasers or bright lights are employed in the process so user complaints and concerns are minimized. Applus+ also uses the iris-scan camera in double duty, capturing a full facial image of the inspector as well as the detailed scan image of the iris. The facial image is stored digitally and attached to the vehicle inspection record, giving additional documentation of the proceedings.

Implementing iris-scan technology in the automotive test and repair environment was a little risky given that no company had attempted such an application on a wide scale in the past. When asked about their reasons for taking the risk, Applus+ Technologies' Executive Vice President, Chris Stock, said, "Connecticut's DMV had expressed a real concern about accountability regarding the inspection of their citizen's vehicles. We looked into fingerprint scanners but were concerned with problems caused by dirty fingers and scanner lens contamination in this environment. When we discovered the research on iris scanners and realized we could achieve an accuracy even better than fingerprint scanning, our minds were made up."

Both Applus+ Technologies and Connecticut's Department of Motor Vehicles are pleased with the benefits of iris-scan technology as opposed the card-and-pass code, but how have the users in the field reacted to the system? "In general, the reaction has been positive," said Jim Valerio. "There is a user learning curve that we've had to work through and some shops complained about that. It's just a matter of getting used to something you've not had to do in the past."

Timothy Collins of Tim's Auto Center in West Haven, Conn., illustrates the point, "I know [the iris scanning] is necessary, but why can't I just type in a password? That would be so much easier."

With the iris scan comes increased scrutiny and accountability for inspectors. Surprisingly, Applus+ Technologies has found that the inspectors are voicing a great deal of support for the increased accountability. "Having this type of authentication makes me feel better about the level of security in the program," says Robert Gould of Darien Auto Center in Darien, Conn. "If I do things right, I will be successful. This prevents guys from cutting corners."

With roughly 900,000 vehicles being inspected in the Connecticut program each year, there are plenty of opportunities for human error in the inspection process. In a typical six-month period 486 violation notices pertaining to various non-compliance activities where issued to inspectors or inspection facilities. The vast majority were minor procedural variances, but minor or not, Jim Valerio says, "Now, in 98 percent of those cases, we know for certain who conducted the inspection and we can target those individuals for remedial training or penalty as the situation may require. We believe this technology is helping to give the motoring public a higher level of certainty that their vehicle inspection was conducted properly."

Thomas J. Fournier is president of Applus+ Technologies Inc., a government contractor that has implemented the iris technology in an operational program.

References

(1) T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report, Issue 1.0," Centre for Mathematics and Scientific Computing, National Physical Laboratory, March 19, 2001
(2) J. Daugman, C. Downing; "Epigenetic randomness, complexity and singularity of human iris patterns,"

Proceedings of the Royal Society of London, Series B, 2001, pp 1737 -- 1740
(3) Iridian Technologies, Panasonic Authenticam Iris Recognition Camera Installation and Operation Guide, September 20, 2001

This article was printed from: **http://www.digitalcommunities.com/articles/Iris-Scan-Authentication-Cuts-Fraud-in-Connecticut.html**