

The Worry and Reality of Liveness Detection

Alan Viars

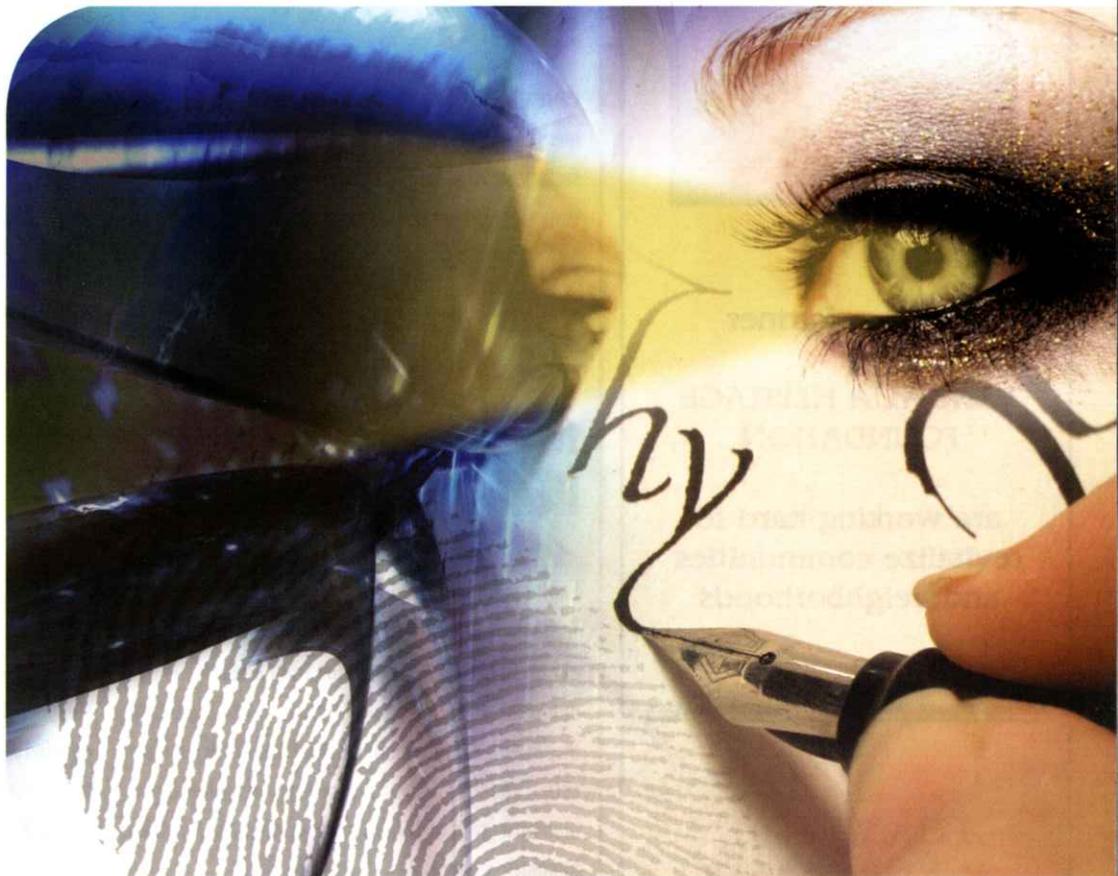
In the movie *Total Recall* one of the 'bad guys' rips an eye from his living victim in order to gain access to a secure area. While such gore may send shivers down our spines in the movie theater, such unspeakable horror is the stuff of nightmares in real life. But never fear, ever so quietly behind the scenes scientists have found a way to combat the physical theft of biometrics.

Liveness detection is any attempt to verify that a biometric sample is from an actual living person and not a cadaver or other artificial object. Many people have demonstrated the ability to circumvent biometric systems by using artificial objects such as rubber hands, "gummy fingers" or photos.

At least a portion of the public is wary of the adoption of biometrics in financial transactions such as ATM

"Techniques to guarantee liveness can work to squelch the public's fear of such gruesome means of identity theft and ease the adoption of biometrics, especially in the financial sector."

machines due to fears of having fingers cut off or eyes gouged out to gain access to some resource such as a bank account.



Methods of Operation

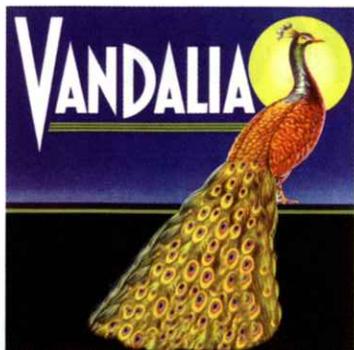
Techniques to guarantee liveness can work to squelch the public's fear of such gruesome means of identity theft and ease the adoption of biometrics. If biometric

verification capabilities were as ubiquitous as Visa-MasterCard, then biometrics could serve to reduce identity theft such as unauthorized use of credit. If

criminals could "steal" biometrics and thus steal an identity, then the utility of the biometric system has been lost.

Still, like biometrics in general, liveness detection is evolving. Furthermore in many applications liveness detection may not be necessary. For example, in a situation where a person, such as a guard, is present during biometric collection, the need for such measures is greatly reduced. It is important for decision makers to look at their own situation and ascertain if liveness detection is required. There is often an additional expense for systems capable of performing some form of liveness detection. An organization must ask itself, "Is the additional investment appropriate for the given situation?"

VANDALIA REDEVELOPMENT CORPORATION



And our Partner

VANDALIA HERITAGE
FOUNDATION

are working hard to
revitalize communities
and neighborhoods

THANK YOU,
CONGRESSMAN
ALAN B. MOLLOHAN
FOR YOUR
EXEMPLARY
LEADERSHIP AND
EFFORTS TO
BUILD A STRONG
FOUNDATION FOR
NORTH CENTRAL
WEST VIRGINIA'S
FUTURE

Techniques for liveness detection vary from modality to modality. Veins may be detected in the face or a pulse may be detected in the finger. Certain biometric systems lend themselves to liveness detection naturally. For instance, liveness detection for iris recognition can flow directly from measuring dilation changes in the pupil and/or detection of blinking. If an organization is considering biometrics implementation with liveness detection, one should ask the vendor about metrics of effectiveness and how the liveness detection was tested.

Spoofing

Currently, liveness detection research and development is taking place both in the public and private sectors. At West Virginia University, scholars from the Lane Department of Computer Science and Electrical

“Currently, liveness detection research and development is taking place both in the public and private sectors.”

Engineering, along with the Center for Identification Technology Research, (CITeR) have taken a closer look at how to accurately determine what biometric is live and what isn't. In its report, *Issues of Live Detection in Biometrics*, they defined the threat or what they call, “spoofing,” as “the process of defeating a biometric system through the introduction of fake biometric samples.”

In research CITeR determined various biometric samples have distinct and traceable characteristics different from a fake or spoofed biometric sample. In other words, for the fingerprint, a reader may be able to detect perspiration or heat; for the iris, the device may be able to detect pupil and eye movement; for the voice, the

reader could match lip movement to the audio; and for the face, the device could detect expression changes. To test this theory, researchers compared live fingerprints to fingerprints from cadavers and molded sources. Using a capacitive fingerprint scanner, CITeR acquired features of temporal perspiration pattern of the skin. Using these features, the algorithm makes a final decision about vitality of the fingerprint. The CITeR research concluded that, “although biometric authentication devices can be

susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks.”

Fool-Proof System?

The risk still exists of being forced to provide a biometric sample by an armed criminal, but this situation exists currently with ATMs. What if a person was given a sleeping drug and then walked to a biometrically-enabled ATM? Multi-factor authentication can mitigate this scenario from occurring. If a card (something you have), a biometric (something you are) and a PIN (something you know) are all required, then a criminal

would be hard pressed to get a PIN from someone who is unconscious.

As the biometrics industry continues to become more and more a part of the main stream, liveness detection will be necessary in many instances, especially the financial sector. Clearly, the key to making the public comfortable with using biometrics is to perfect liveness detection. ☺

Biofact

Demand for identity and access management software grew by 10 percent to reach \$719 million in 2004. And the industry research group predicts the market will almost double again in the next five years to hit \$1.3 billion in 2009.

Source:
IDC: <http://www.idc.com>