Face Authentication for Password Replacement

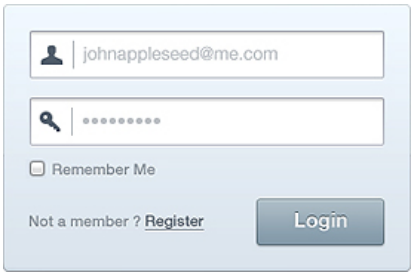
Ver-ID is a client-based face authentication software created by Applied Recognition. It can operate on all Windows and Mac desktops, as well as Android, iOS and Blackberry mobile devices. It is designed to integrate with existing password-based systems, simple for any business looking to add face authentication security to SaaS, Cloud, Web or independent applications. Running locally on a user's device, Ver-ID provides a second factor of authentication by taking advantage of "Something You Are" biometrics. Ver-ID security can also be augmented with "Something You Know" verification, should it be warranted.

Ver-ID face authentication demo for iOS showing anti-spoofing and ID capture.

Credential Capture

Virtually all government-issued identification includes a photo, the most common being a driver's license. As part of the Ver-ID registration process, a photo is taken of the user's ID along with the user's live face and a comparison is done between the two. This method not only strengthens Ver-ID's face recognition accuracy, but also helps institutions adopt face authentication as a trusted method of identity confirmation.

Password Replacement



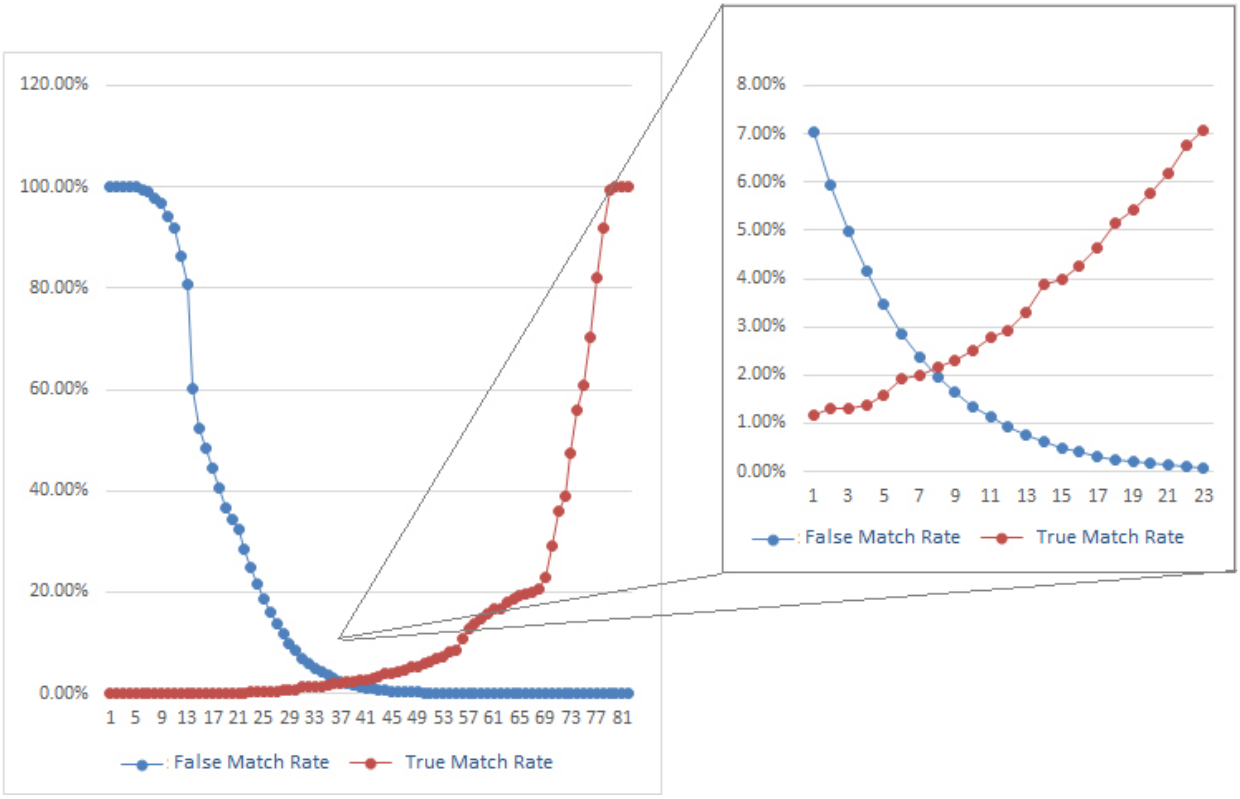
As previously mentioned, Ver-ID integrates seamlessly with existing password-based systems. Face authentication can be used to replace the traditional password login, augmenting protection by delivering encrypted passwords to an array of apps or servers. Ver-ID can also be used as a second factor authentication for more secure applications. The conversion to biometrics doesn't have to be complex. The Ver-ID demo app shows proof of its simplicity, enhanced security measures and time-saving user interface; saving the hassle of forgotten passwords and account lockouts.

User Controlled

The tech world has always had issues with password security. Biometrics are proving to be a very effective solution to this problem. Applied Recognition has designed Ver-ID as a client-side solution where personal biometric information remains on the local device. The key benefit of the Ver-ID approach is its compliance with recent government legislation in the US, EU and other countries that block collection of personal biometric data on central servers. An additional benefit is that there is no single repository of biometric data for hackers to attack.

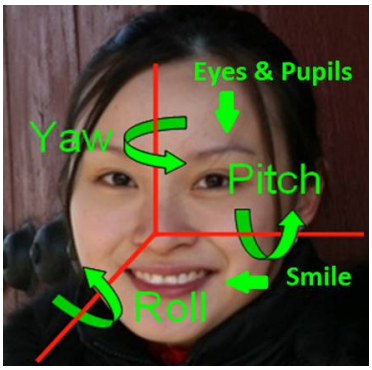
Friendly and Secure

There is a trade-off between ease of use and tighter security; the higher the security level, the more difficult a program is to use. Ver-ID allows you to control all aspects of initial registration and subsequent authentication sessions. Depending on the security needs of the application, settings can be altered for easier interaction or enhanced security.



Anti-spoofing

Every tech security company anticipates hacker attempts to undermine their system. For face authentication, this typically involves the use of a picture or a high definition video to spoof a registered face.



Ver-ID is designed to eliminate this type of activity by employing a number of anti-spoofing measures which can be set based on the security needs of the application. Similar to how CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) works to prevent computer bots from accessing websites, Ver-ID reaches beyond this to validate live users and prevent fraudulent access by humans or computers.

Our methods include detection of random movements and expressions of a user that serve as proof of a live person in front of the camera. These detection methods can be employed automatically in the background of an application, or on demand for one-time authentication. Options include asking users to smile, move their head in a specific direction, etc. in random combinations.