STONELOCK

Revolutionizing Identity Protection With Near-Infrared Facial Recognition

A StoneLock White Paper

The Problem

Both business and government institutions struggle to deploy swift, simple, reliable, and cost-effective solutions for identity management and access control. Fingerprint readers, swipe-able badges, and combination keypads all suffer from common security issues – most notably that they can be "spoofed" allowing identity validation or granting access to the wrong person, or to more than one person at a time. Conventional camera-based facial recognition systems can similarly be spoofed to allow validation and access to unauthorized persons.

StoneLock is the designer and manufacturer of a near-infrared (NIR) facial recognition access control product based in Olathe, Kansas (www.stonelock.com). StoneLock is recognized as a best-in-class biometric solution suitable for the most critical identity management and access control situations, tested and vetted by many of the most sophisticated enterprise security customers in the world – to include banks, airports, and data centers. StoneLock's speed (< 1 second authentication, accommodating typical turnstile rates of approximately 40 people per minute) and accuracy (better than .0004% FAR) make it suitable for critical applications in both commercial and government settings.

With an eye toward simplicity and best practices for privacy and compliance, StoneLock's template files contain no personally identifiable information (PII). A StoneLock template is a data file that does not resemble the user in any way, and cannot be used to identify any user without a StoneLock device and the user present. *Only a live read of a user (who has opted into the system) can match a StoneLock template with the user*. The authorized user's face is that person's unique access key. Although it can be, and often is, combined with two factor or even three factor authentication, the StoneLock NIR facial solution allows for portability, simplicity of operation, and speed without creating a burdensome PII compliance regime on the back end.

In short, the StoneLock solution improves security, increases secure access throughput, has greater accuracy than existing solutions, and can be used to address a variety of enrolled populations.

The StoneLock Difference

StoneLock's facial recognition accuracy relies on the consistent measurement of facial features. StoneLock is designed from the ground up as a near infrared (NIR) spectrum solution. Near infrared, as opposed to full infrared, provides a cost-effective alternative to the visible wavelength design while providing an immediate improvement in performance. To reinforce a NIR biometric capture, StoneLock incorporates an infrared LED array that works to minimize the impact of ambient light on capturing facial uniqueness – resulting in the ability to operate in an ambient light environment between total darkness and just short of full direct sunlight. Both the camera and the LED array are packaged into a dedicated edge device mounted at the location of the verification requirement. This makes StoneLock solutions both standard and stable across a number of application environments.

Other biometric systems vary widely. Their differences in performance can be attributed to:

- ***The intent*** of the biometric system. Is the system designed to identify faces in YouTube videos or on a casino security cam? Is the subject/user cooperative? How transparent do you want this experience to be for the user? How many users will you be processing? How will you enter users into your system? These constitute but a few of the design considerations of a biometric system.

- ***The design***, with component systems more often than not designed by different engineers, with different instructional mandates, coming from different disciplines at different points in time.

- ***Inherent limitations*** in various components, such as a commonly-used public domain algorithm or a certain type of sensor, in the lifespan of components and the inherent limitations in the entirety of the biometric itself.

The face is the most unique of the physical features that establish identity. Many non-infrared facial recognition algorithms are designed to work with current security video monitoring systems, attempting to identify a face reliably from a photograph or video frame, perhaps at a distance or in a crowd, or even from someone who may not want to be identified. For both intrinsic and extrinsic reasons, those types of facial recognition are difficult to manage and do not achieve very high accuracy - typically testing in the 45-65% range. In an environment where failure is not an option, even 75% success is not acceptable.

These variables all play significant role in the performance accuracy and reliability of every non-infrared biometric system on the market today. StoneLock overcomes that variability by providing a solution that is standardized at scale, technically superior, more accurate, faster, more configurable, and cost effective.

Key Technical Elements

As a dedicated edge device, the StoneLock reader's exclusive function is to create a near-transparent experience for the user during the reception of face information. The hardware is tailored to the specific requirements of quickly and intuitively guiding a user's approach and recognizing faces.

NIR wavelengths are safe, invisible to the eye, and relatively unaffected by ambient light or temperature. NIR penetrates biological tissue deeper than visible light, allowing for sub dermal spectroscopic measurements ideal for capturing intrinsic properties (shape, reflectivity, expression) while minimizing unfavorable extrinsic factors.

The StoneLock Pro biometric access control device consists of a faceplate and control unit. Visit www.stonelock.com/resources/ for tech specs

The implementation of NIR technology immediately provides a boost in performance over the industry standard. But simply mounting a device at a convenient spot on a door is not enough to achieve optimal alignment while also being as transparent as possible to the user. Both users and operators want a ***transparent*** solution – that is to say, as non-invasive as possible. For example, identity validation enrollees don't want to be inconvenienced by a disruptive verification process that requires higher levels of active participation (such as alignment - and not blinking – during an iris scan). At the same time, those administering an identity validation program expect the highest levels of identity assurance and protection for an enrolled population. Security operators recognize systems that are transparent to the user as having a distinct advantage over systems that introduce annoyance or frustration. The fact is: *user adoption and compliance, both conscious and unconscious, is vital to the success of any security system*. And that's exactly where StoneLock excels as a reliable solution. To achieve this, StoneLock incorporates key design elements:

- **Transparency.** *If you can use a mirror, you can use StoneLock.* In order to ensure proper reads, StoneLock's socio-technological interface design enlists help from basic human behavior in the user interface. Mirrors act as "animal magnets." All animals – including humans - respond to mirrors. The immediate response for all animals is to walk towards the mirror and

look into it. StoneLock leverages this 'mirror effect' to help deliver a transparent user experience in the design of the edge device.

A second visible camera was added to the device and a small monitor was added to show the user their image. When a user sees their image on the screen, the mirror effect encourages the user to center their face, looking full forward, to best view one's own image. This allows StoneLock to capture a precise, close, full frontal image, improving its ability to capture uniqueness. Typically, StoneLock's application of the mirror effect draws the user into perfect alignment resulting in an optimal solution performance: matching accuracy in excess of 90% with less than one second of user interaction with the system.

- **Facial Points and Diminishing Returns.** The gathering of facial data points, like all data sampling techniques, suffers from diminishing returns. Taking points on cheeks provide minimal uniqueness gains and the number of eye points that can be captured is limited. StoneLock determined that 2,165 was the optimal number of points that minimized diminishing returns in matching accuracy.

  Further, StoneLock implements a proprietary new type of point analysis called Layered Reinforcement. StoneLock takes the image of a face and overlays several layers of different size pixel boxes on the image. The layering of pixel boxes of different sizes has an amplifying impact on the analysis of the face. Areas that are exceptionally unique to the face are emphasized, and areas that are more common between faces are deemphasized.

This 'layered reinforcement' of the unique characteristics of the face is proprietary to StoneLock technology. As a result, StoneLock has a distinct advantage over other facial recognition biometrics in two key areas:

- *First*, the algorithm performance improvement boosts StoneLock above the 90-percentile range for overall performance – a standard much more accurate and reliable than the roughly 45-65% accuracy of other solutions.

- *Second*, StoneLock technology can handle a large number of users distributed to the edge, as opposed to centralized processing of user data. As centralized processing systems work to improve performance by adding non-layered points to their sampling, the workload on the servers performing the analysis increases, requiring upgrades to more powerful processors in order to increase the users processed. StoneLock solves this with a clustered processing architecture, distributing workloads and managing data for maximum system efficiency.

The Problem Solved!

StoneLock's unique NIR facial recognition overcomes the security and operational shortcomings of other identity validation and access systems, including non-infrared facial ones. StoneLock all but eliminates the need for separate manual checks, providing a true end-to-end solution for industry and for government. StoneLock improves security, while at the same time providing a fast, easy and reliable experience for both administrators of, and enrollees in, identity validation and access control systems. StoneLock can handle large numbers of people and scale with high accuracy. All while keeping system installation and maintenance costs in check.

StoneLock is continually expanding its product offerings, soon allowing for global credentialing and ensuring seamless identity assurance from anywhere in the world. StoneLock's unique approach to biometric credentialing has established proprietary architecture that meets the ultimate challenge of identity management and access control while establishing NIR facial recognition technology as a viable global identity standard.