Ultrasonic Biometric Authentication / Verification in Mobile Devices

Description of the Value of Biometric Authentication in Mobile Devices

Everyday hundreds of millions of people use mobile devices to help make their lives easier and more convenient. Before using their phones, however, most type in some kind of passcode. Additionally, before using many third party applications, users are required to enter an additional user name, password, and often other information. Applications that require some type of authentication and / or verification include mobile banking, e-commerce providers, downloading applications, wireless providers, and numerous other vendors. These authentication and verification steps are a critical component of mobile security, yet slow down users and can make it impossible to perform tasks if users forget part of their login information. User names and passwords are also prone to hacking and theft.

Many of the world’s leading technology companies such as Apple, Microsoft, and Google are working on incorporating biometrics into mobile devices, yet despite installation on over 100 million devices biometric security is not yet widely accepted. Most of the current devices with biometric technology include a fingerprint scanner on the back of the phone. These optical scanning devices are unreliable and often produce errors which are unacceptable in critical use cases such as financial transactions. Optical fingerprint scanners take pictures of the ridge structure, but the images are often blurred by dirt, grease, oils, and other
contaminants. These pictures are even worse on mobile devices that are constantly handled and placed in bags or pockets.

A biometric solution that could easily, quickly, and accurately identify users would not only improve user experience but also make mobile devices more secure. Fortunately, this technology was recently developed and could change the way users verify who they are on mobile devices. A company called Ultra-scan recently developed a technology called ultrasonic fingerprint identification which uses sound waves to see through skin, fat, and other tissues. Ultrasonic technology has been used in medical applications for decades with the most common being fetal imaging. Ultrasonic waves allow for high quality images in spite of any contaminants. Ultra-scan has developed a new system that has passed the most stringent government tests including FBI benchmarks. From the Ultra-scan press release announcing the breakthrough,

“Ultra-Scan Corporation, the global leader in ultrasonic imaging and sensor technology, announces the receipt of FBI Appendix F certification for its groundbreaking Thin Film Transistor (TFT) fingerprint sensor, which integrates the sensing layer with the imaging layer facilitating packaging into a variety of mobile device technologies for performing secure electronic fingerprint enrollment and authentication.”

This new technology is essentially a thin screen (less than 1.0mm) and accompanying software that can detect the critical points on a fingerprint with extreme accuracy. Once Ultra-scan detects a fingerprint it can be checked against existing fingerprint databases. The technology has been tested with existing cellphones and works well. It adds less than $10 to the cost of a phone and is easily incorporated into existing manufacturing processes. Ultra-scan
developed the technology as part of the $30M research and development project and is currently looking at commercialization and licensing opportunities.

Value Blueprint / Ecosystem

An ultrasonic biometric authentication system on a smartphone provides a tremendous value proposition to end customers and the innovators, but it is important to assess the value given to each player in the ecosystem that is required to adopt this innovation in order to make it successful. For this innovation, both hardware and software adoption are required. Figure 1 shows the value blueprint for the adoption of a biometric authentication system on a smartphone.

![Value Blueprint for Biometric Authentication Ecosystem](image)

**Figure 1:** A value blueprint for the biometric authentication ecosystem in phones

The suppliers of this innovation are thin film transistor manufacturers (e.g. Corning) and component suppliers of ultrasound technology. The intermediaries of this innovation are OEMs (e.g. Samsung, Apple, HTC, and Nokia) on the hardware side and mobile operating systems (e.g. Google for Android, Apple for iOS, and Microsoft for Windows Mobile) on the software side. The suppliers to these intermediaries also include the assemblers of the devices. The key complementors for this innovation are service providers that require authentication to access
their services (e.g. banks, trading platforms, email services, electronic medical record holders, etc). The suppliers to these complementors are application developers for the mobile operating systems.

Co-Innovation Analysis

In order for Ultra-scan’s technology to be successful, it is critical to first look at what other technological developments are necessary for the technology to succeed, the co-innovation analysis. Fortunately, Ultra-scan’s technology only requires slight modifications of technologies of other players in the ecosystem. The software to run the fingerprint detection requires a small additional microchip that will need to be installed into mobile form factors. This chip is simple to design and manufacture and can be produced on existing semiconductor manufacturing technologies. Also a component manufacturer will need to develop a process to produce the Thin Film Transistor (TFT) components. This is an easy process and should not cause any difficulties. There is a slight innovation risk with the OEM’s as they need to find a way of integrating the thin film transistor and the additional chipset into the design of the phones, while keeping the form factor, battery life, and performance intact. Ultra-Scan has successfully produced prototypes, and this is expected to be an execution challenge that the assemblers and Ultra-Scan are able to overcome. Finally, the software needs to be added to mobile operating systems and API’s need to be available to application developers so they can use the new system. While this is not a trivial task, mobile operating system companies work on projects like this every day so there should not be a technological innovation barrier. In order for Ultra-scan to be successful, there are not any red lights with respect to co-innovation risk.

Adoption Chain Analysis
A second key element of Ultra-scan’s success will be whether the other members of this ecosystem adopt Ultra Scan’s biometric solution. The suppliers of the hardware component of Ultra-Scan’s solution must agree to make this new product. Since this is in line with what they are already doing the risk is low, green light.

The next actor in the chain is the phone assemblers such as Foxconn. The adoption risk here is minimal as the decision maker in this process is the OEMs. If the OEMs believe that end customers will gain value from a new technology they will work quickly to incorporate these new innovation into their products as differentiation among mobile hardware is becoming ever more elusive. The assemblers will do what the OEMs request, as long as they are financially rewarded for their work, green light.

The OEMs present a bigger risk. OEM’s incur several costs in adopting this solution, including the added complexity in assembly and chip design, the increased risk of failure due to additional components, and the time needed to create this change. To adopt this solution, the benefits to this change must offset all of these. The benefits will come in one form – increased revenue through higher volume of handsets sold or the mitigation of lost revenue through handset substitution if other OEMs pick this product up. The driver of higher handsets sold will be a customer driven demand for, not just for Ultra-Scan’s product, but the ecosystem adoption of this product. Therefore, OEMs will only adopt if the rest of the ecosystem adopts, but will not lead the charge, yellow light.

Analysis of the OEM’s behavior is further complicated by the financial and operational ties between the OEMs and the mobile operating system owners. In some cases they are the
same actor (Apple) and in others there are very strong dependencies (Samsung and Google or Nokia and Microsoft). In most cases, the power lies with the mobile operating system as it has scale with and direct impact on the end customers.

The adoption risk is low with mobile operating system companies as the biometric authentication solution becomes a clear differentiator for these players in providing security solutions embedded within their ecosystems. Adopting this authentication solution allows these agents to advertise their operating systems as more secure to both consumers and enterprises, green light.

The last element of the value blueprint is the service providers that will use the authentication solution to allow consumers access to their services. The adoption risk here is a red light as these service providers have no incentive to adopt this new solution. Here lies the key constraint in the adoption chain. Bank of America, for example, is one service provider this authentication solution would target. Currently its authentication on mobile devices is the same as authentication for websites – a simple password. However, it has rolled out a system called SafePass, which is a second step authentication system required for any bank transfers. If and when Bank of America deems it necessary to upgrade sign-in procedures to a two-step authentication system, it would choose to extend SafePass – a system it knows and that is scalable rather than a new system which it would have to integrate with its back-end processes and then roll out. The cost of adoption is simply too high.

Ultra-Scan’s strategy for adoption with end customers has to look at service providers outside the traditional ones that use established authentication methods. In time, as adoption
occurs the traditional actors will take a second look at the biometric solution and consider adoption.

Two companies that Ultra-Scan should target together with the mobile operating systems are Paypal and LevelUp. Both companies hold confidential customer information, service mobile payments, and require cumbersome log-in procedures in times of high stress (standing in queue deciding what to order then realizing you have to pay but log in first). LevelUp gets around this by allowing a permanent logged-in feature, but this makes its service less secure in case a customer’s phone is lost or stolen.

The value proposition to both these companies is big. Both companies are trying to scale up mobile payment services and the combination of convenience, security, and speed are some of the barriers to adoption within that ecosystem. A biometric authentication system which locally validates based on a simple finger press makes for a simple and secure authentication process and these companies would be willing partners.

The history of new technology launches in mobile operating systems, especially with iOS, indicates that what is needed to drive mass adoption is a couple of very compelling use cases that demonstrate the simplicity and functionality of the new technology. This has been seen with Apple’s launch of retina display, notifications, siri, and countless others. Paypal and LevelUp will be the use cases for biometric authentication and will spark the use of this authentication technology in a plethora of other apps driving adoption by the OEMs.
A final key point is that Ultra-scan should not be the leader of this ecosystem. The leaders of this ecosystem are the mobile operating systems, but the key constraint lies with the complementors – the service providers who will commission apps to use the authentication service. Everyone else in the ecosystem will adopt once the mobile operating systems launch the service and the use case is demonstrated. Ultra-scan must focus its alignment efforts on bringing in an ecosystem leader such as Apple, Google, or Microsoft and then working with them to shape the ecosystem to bring a benefit to the service providers. Without changing the value proposition for the service providers this technology will fail in the marketplace.

First Mover Analysis

From the adoption chain analysis it is clear that Ultra-scan should not be leading this ecosystem, yet it is still important for them to understand what is necessary to be successful. One critical aspect to analyze as an innovator is what, if any, relative advantage you get from early entry into the market. Since Ultra-scan’s innovation execution challenge was difficult and the complementor co-innovation challenge is low there is an increased level of first mover advantage. It is not as high if the innovator execution challenge was low, yet Ultra-scan should still move quickly to become a member of a new biometric ecosystem. Major technology companies are working on creating this ecosystem and if Ultra-scan does not move quickly it could easily be replaced by another technology. In order for Ultra-scan to succeed, it must convince a potential ecosystem leader that it can be the best technology player to include in the mobile biometric authentication ecosystem.