WHITE PAPER

Hardware Obsolescence Management in the Biometrics Industry

REDUCING COSTS BY ENHANCING THE FLEXIBILITY OF BIOMETRIC SOLUTIONS

AWARE

Hardware Obsolescence Management in the Biometrics Industry

REDUCING COSTS BY ENHANCING THE FLEXIBILITY OF BIOMETRIC SOLUTIONS

"Hardware obsolescence" is a term used to describe the eventual unavailability of hardware product models resulting from the introduction of new products of the same purpose. It is typically brought about either by technology improvements or new functionality and performance requirements of the marketplace. In complex systems, hardware obsolescence can add substantially to the overall cost of device support and maintenance over its lifetime. Costs associated with hardware obsolescence are unpredictable; they are difficult to measure, quantify, and budget for. This paper addresses hardware obsolescence in the biometrics industry, and offers solutions that can help mitigate these costs and uncertainties.

Technology product life cycles can be quite short; particularly those addressing nascent or evolving markets, such as biometric capture hardware. Biometric capture hardware products—such as fingerprint live scan devices, fingerprint card scanners, iris cameras, and digital cameras—are used for biometric enrollment, and are typically controlled by a software application running on a host workstation. Capture devices require a software component or interface such as an API or driver provided by the manufacturer to be exercised by the user interface layer of the application in order to control them. When a proprietary software interface is used to operate a device, the software application can only function properly with a software component provided by the hardware provider.

In some cases, technology standards are drafted and implemented to mitigate the obsolescence problem by specifying universal interfaces that attempt to achieve interoperability of a software application with multiple hardware devices. However, standards may have life cycles longer than those of the products they attempt to address (five years or more), and can fall behind the state of the art, constraining product functionality and performance. These standards can also tend to apply to the "least common denominator" of the features and capabilities of different vendors, preventing the user from taking advantage of differentiating and innovative features of various devices.

When unmanaged, the use of proprietary interfaces causes interdependencies between the software application and capture hardware that are costly and difficult to anticipate and plan for as a deployed solution ages. The problem is exacerbated where high throughput, harsh environments, or other demanding usage conditions reduce device reliability, and further shorten the life expectancy of hardware products. This can require frequent or unpredictable device replacement, as is sometimes the case in large-scale biometric capture systems.

Interdependence between the hardware device and the software application layer can be costly for several reasons. The primary reason is that once a software application has been developed around a particular hardware device, the owner of the solution is relegated to utilizing that device from that vendor. This means losing access to a competitive marketplace offering a growing variety of devices of equal or higher performance levels at lower price points. One alternative is to design an application to use software from multiple hardware vendors, but this builds costly functionality redundancies into the software application, and creates differences in workflow and look and feel, depending on which device is used.

Hardware models can also go out of production or be replaced by an incompatible model. A solution owner can find themselves in a position where they prefer a different hardware offering or are compelled to change models, but options are not available to them without a potentially costly and disruptive modification to their software application. This can require expensive and risky software upgrades, modified workflow, user training, and other potentially expensive problems resulting in downtime.

Case in Point

Fingerprint capture with live scan devices

"Live scan" devices apply advanced optics to fingerprint capture. Digital fingerprint images are used to perform biometric verification and identification by extracting "minutiae" features and mathematically comparing them to other samples. In order to achieve sufficient performance levels in terms of false match and non-match rates, a high-quality, high-resolution, high bit-depth image must be acquired. For this reason, the FBI defines strict quality requirements to which live scan hardware must adhere, called the Image Quality Specification, (IQS) included in "Appendix F" of the EBTS standard. Appendix F identifies minimum imaging quality requirements such as resolution and gray bit depth, among others. Every hardware device must pass tests by an independent party to achieve compliance to this specification and to be used to submit prints in compliance with the EBTS specification. As a result, every Appendix F-compliant hardware device produces raw imagery of sufficiently high quality that is roughly equivalent to each other in terms of minimum raw image quality.

But raw images are not suitable for biometric applications. They must be compressed with FBI-certified WSQ image compression software, and must not be over-compressed. Most importantly, the content of the image must be of sufficient quality to be useful. That is, the images of the prints themselves must have enough information to be used by the matching system. The better quality the content, the better performance can be achieved, which means fewer false matches and misses. Fingerprint images must fulfill a long list of requirements

Hardware obsolescence with digital cameras for facial image capture

The hardware obsolescence problem is even more pronounced for consumer-grade digital cameras traditionally used for biometric facial image capture, largely because the product life cycles for these cameras are even shorter than for live scan (on the order of twelve months.) Furthermore, because the requirements for biometric facial images can be stringent (see ISO/IEC 19794-5), it is very useful to enable software to externally perform pre- and post-capture analysis and processing analogous to the fingerprint capture techniques previously described. For this purpose, it is useful to be able to control zoom, autofocus, flash, brightness, shutter, and other camera functions from software running on the host workstation CPU again, in an analogous fashion to fingerprints.

But not all cameras provide access to these functions, particularly in the lower end of the product spectrum. In fact, some camera manufacturers are discontinuing support of external control of their lower-end consumer-grade cameras. For example, while Canon had previously supported such capability in its "PowerShot" line of cameras, which can be purchased for on the order of US $200, compatibility between their SDK and the PowerShot line ended in 2009. Now only its EOS line of higher-end SLRs can be operated via the API provided in its SDK.

For this reason, it is anticipated that industrial cameras will increasingly be used for biometric facial capture applications going forward. These cameras offer longer life cycles and a high degree of external control capability, but also a more fragmented market, supplied by smaller, more specialized players. In the long term, this will be a positive turn for facial biometrics, but the transition will have a learning curve; industrial cameras are sold quite differently from consumer-grade cameras. For example, housings and lenses are often sold separately, and the cameras can tend to be more expensive for similar resolution and image quality. There are wider variations in pricing from different vendors and for different volumes, and high-volume purchases are often the norm for these products.

In short, camera abstraction is just as important for a biometric capture system as is fingerprint live scan abstraction. The reasons are the same; efficient life cycle maintenance of the system, independence from the device vendor, and ability to implement common quality assurance criteria.

to be useful, and software should be used to assure these requirements are fulfilled to the extent possible for each fingerprint enrollment:

- Images must not be too light or too dark, in order to have sufficient "ridge flow". In other words, fingerprint ridges—the source of the identifiable features, or "minutiae"—to the extent possible should not be broken along their length, and should not be joined with adjacent ridges.
- Fingerprint images should not deviate significantly from 90 degrees (perpendicular to the sensor). High angular deviation from 90 degrees requires the matcher to realign the image to 90 degrees, which can introduce a loss of precision.
- Fingerprint images must consist of flat impressions or "rolls" of the central region of ridge flow on the finger pad. They should not consist of partial prints or side impressions which can eliminate the capture of the significant landmarks in the print such as the core or deltas.
- Multi-finger images, or "slaps", must yield independent images for each finger. That is, they must be properly "segmented".
- Fingerprint images must be captured in their entirety; that is, they must not be touching the edge of the sensing area of the scanner.
- The source of each fingerprint image must be properly identified. That is, which hand and which finger each print is from. If fingers are misidentified they cannot be matched.

This presents a challenge—particularly in a high-throughput environment—because it is difficult to distinguish these problems with the naked eye. With image processing software, novel techniques can be employed to ensure that each print is properly identified; these include identification of the "handedness"—left or right—of the slap image, identifying incorrect matches between prints of different fingers, and identifying incorrect non-matches between rolled images and slap images of the same finger.

While hardware performs capture of raw, unprocessed digital fingerprint images, advanced image analysis should be performed by software algorithms running on the CPU of the host workstation, operating largely independently from the hardware in two modes: pre-capture and post-capture. During pre-capture mode, the workstation imports a live stream of raw images from the scanner. During this process, the software is performing analysis on a lower-resolution version of the image stream to identify problems with the image, such as low ridge flow, high angle, wrong hand, unsegmentability, or a finger touching the edge. Once all the quality thresholds or criteria are met, the hardware device can be triggered to perform capture of a full-resolution image. The resulting full-resolution image is again analyzed during the post-capture process to ensure sufficient quality using a quality algorithm such as the NFIQ (NIST Fingerprint Image Quality) algorithm and several other quality tests. A good enrollment system should make multiple different quality measures and utilize more than one quality algorithm. Each quality algorithm is different and makes different sets of analyses. When two quality algorithms produce contradictory results for a given image, the system should support a workflow that flags the image for further investigation or recapture.

Live scan vendors typically offer software that runs on the host workstation CPU to perform some subset of this functionality. This software offers a proprietary application program interface (API) that enables it to be incorporated into the application layer of the solution. But this software operates only with the hardware device for which it is designed. This renders the application reliant exclusively on the device being used.

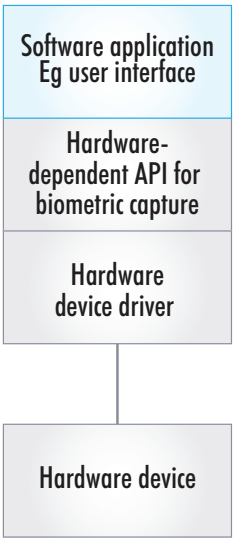
Addressing the Problem

Hardware abstraction

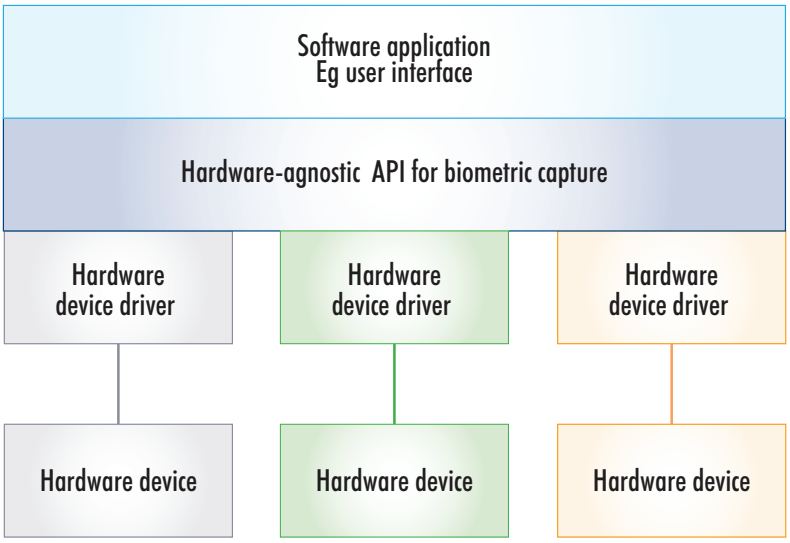
In the case of fingerprint capture, interdependence between software and hardware is largely unnecessary because the actual interplay between the host software and the hardware device is quite straightforward in terms of interface complexity; while there is advanced image processing required on the host, all the image processing application needs from the device is 1) unencumbered access to a real-time, raw image stream, and 2) the ability to quickly trigger a capture of a full-resolution image. With access to the real-time raw image stream, the powerful CPU of the host device can be put to task to perform advanced pre- and post-image analysis and highly effective fingerprint capture as earlier described.

Reliance on a particular hardware vendor can be eliminated by utilizing fingerprint processing software that operates equivalently and independently from a wide range of hardware products. Instead of using soft-

Use of hardware-dependent API for biometric capture



Use of hardware-agnostic API for biometric capture



ware from hardware vendors to perform biometric image analysis and autocapture functions, the device is abstracted at the driver level. The software component from the hardware is replaced with a component from a third party that 1) performs the required image autocapture and pre- and post-capture processing, and 2) interfaces with the APIs of many hardware devices, adding new device interfaces as they become available on the market.

Removing interdependence between the software application layer and the hardware device has powerful implications:

1) The solution owner is able to develop, upgrade, or otherwise modify their application without restrictions imparted by limitations of a particular hardware device.

2) The solution owner can use different hardware devices in the same system with the identical software application and workflow, and with the same quality assurance criteria

3) Operators can be trained to use the same application interface and workflow, without differences caused by different hardware devices.

4) The solution owner can source hardware devices from the entire competitive marketplace, and benefit from the reduction in risk associated from dependence on a single vendor.

5) The solution owner can replace hardware devices of a legacy vendor with products from other vendors that might present better functionality, performance, or cost.

6) The same software application can support the use of different hardware products in varying usage conditions.

Quantitative Model

Capture hardware deployment and maintenance

The following is a quantitative model that represents a deployed biometric solution utilizing 1000 capture workstations with hardware devices. It illustrates the complexity of managing a large deployed base of hardware, with product life cycles (rate of introduction of new models, rate of model obsolescence) and product life expectancy are identified as follows:

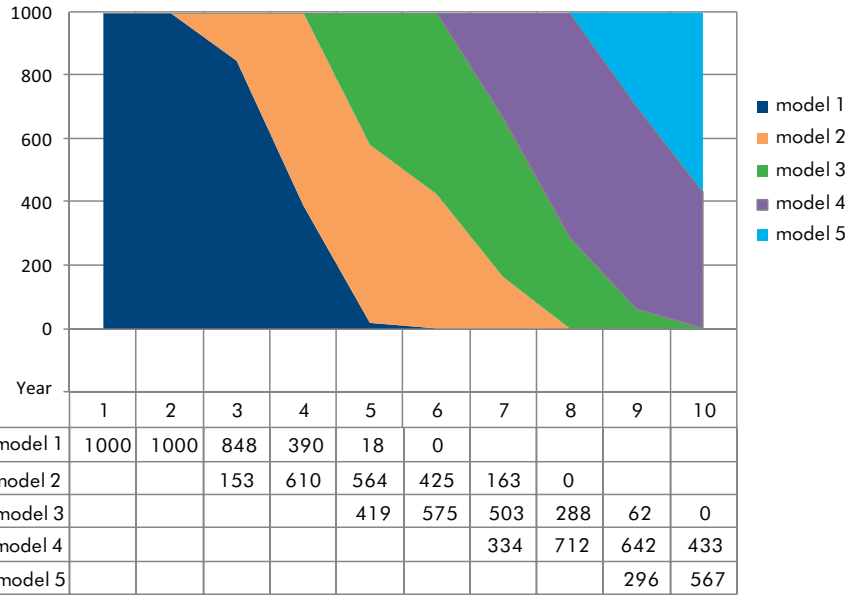
1) Product life cycle of two years (new products introduced to the market and replacing previous models every two years)

2) Product life expectancy of five years, with the likelihood of a device requiring replacement in a given year of its lifetime is as follows:

a. Year 1: 0%
b. Year 2: 5%
c. Year 3: 15%
d. Year 4: 45%
e. Year 5: 35%

The diagram in Figure 1 shows the composition of the described biometric capture network in terms of hardware models. In Year 1 of the deployment, there are no equipment breakdowns. In Year 2, 5% of the hardware devices fail and are replaced with the original vendor and model. In Year 3, a new model is introduced with changes to the hardware device and accompanying software. 15% of the units deployed in Year 1 fail and must be replaced with Model 2. In Year 4, an additional 45% of the units deployed in Year 1 fail, along with 5% of the Model 1 devices deployed in Year 2 and are replaced with Model 2. Even with perfectly (and optimistically) predictable failure rates, new hardware models must be introduced into the system in a haphazard and "lumpy" frequency, requiring support for up to three different models at any given time.

As illustrated by Figure 2, the majority of equipment replacements must be performed with model upgrades as opposed to equivalent models. As discussed, introducing new hardware models, particularly with reliance on an associated software modification or upgrade, introduces often unanticipated costs and complexities to a system. Complete disassociation between the software application and the hardware device mitigates the problem to a substantial degree.



Year	1	2	3	4	5	6	7	8	9	10
model 1	1000	1000	848	390	18	0				
model 2			153	610	564	425	163	0		
model 3					419	575	503	288	62	0
model 4							334	712	642	433
model 5									296	567

Figure 1: Composition of biometric capture hardware system over time

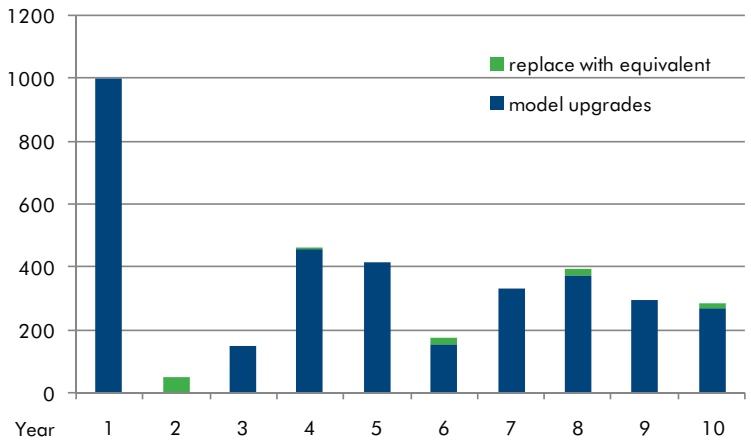


Figure 2: Capture hardware replacements

Summary

Hardware obsolescence contributes unpredictable costs and risks to the ongoing maintenance of a complex biometric system. Driver-level abstraction of capture hardware devices can mitigate these costs by eliminating interdependencies between the user interface and the devices, allowing a much higher degree of flexibility in selecting device vendors and models as devices fail over time. Designing a biometric capture application to utilize a modular autocapture/QA software component establishes equivalent quality assurance criteria across different hardware devices and maintains compatibility with new devices as they become available.

About Aware, Inc.

Aware is a leading provider of commercial off-the-shelf (COTS), standards-based biometrics software since 1992. Our products enable solution providers and system integrators with interoperable, standards-compliant, field-proven biometric functionality for applications including credentialing, border management, and criminal justice. Aware continues to build upon this legacy as a leading provider of innovative, high-quality, state-of-the-art biometrics software. Our client- and server-based software tools and applications enable integrators, solution providers, and government agencies to analyze, optimize, compress, format, match, store and transport biometric images and data according to international standards. End users include federal, state, and local government agencies such as the FBI and other U.S. Department of Justice agencies, the U.S. Department of State, the Department of Homeland Security, and government entities throughout Europe, Asia, and South America. More can be learned about Aware's products at http://www.aware.com/biometrics.

AWARE

The information presented in this document is designed as an introduction to the Aware suite of biometric tools. If you would like further information, extended examples, or product manuals, please contact Aware at:

help@aware.com
www.aware.com/biometrics