INTEGRATED BIOMETRICS

Little Fingers. Big Challenges.

How Image Quality and Sensor Technology Are Key for Fast, Accurate Mobile Fingerprint Recognition for Children

The Challenge of Children's Identity

While automated fingerprint recognition for adults is an established practice on a global basis, children represent a considerably more ambiguous area. Typical concerns include:

- Whether the changes in finger structure as children grow impact the ability of matching systems to verify someone years after their initial enrollment
- The smaller size of a juvenile fingerprint and if it provides sufficient information for accurate enrollment and matching
- Poor image quality due to physical restlessness, shorter attention span, unclean fingers, or similar behavioral factors common to childhood

> *Given that very young children are often uncooperative and do not comprehend or follow instructions, in our opinion, among all biometric modalities, fingerprints are the most viable for recognizing children. This is primarily because it is easier to capture fingerprints of young children compared to other biometric traits, e.g., iris, where a child needs to stare directly towards the camera to initiate iris capture.*[1]

In 2013, the Joint Research Centre (JRC) of the European Commission released a research report to answer these questions.[2] The JRC report's opinion is that "under appropriate conditions, fingerprint recognition of children aged between 6 and 12 years is achievable with a satisfactory level of accuracy."

A more recent study at Michigan State University expressed even greater confidence in biometric fingerprinting for children, asserting that, "fingerprints acquired from a child as young as 6 hours old exhibit distinguishing features necessary for recognition, and that **state-of-the-art fingerprint technology achieves high recognition accuracy … for children older than 6 months**."[3] [emphasis added]

Acceptance is another factor in weighing the utility of biometric fingerprint recognition for children. A recent survey conducted by the Center for Identity at the University of Texas at Austin demonstrates a distinctly higher rate of acceptance for fingerprint scanning over

---

1 *Biometrics for Child Vaccination and Welfare: Persistence of Fingerprint Recognition for Infants and Toddlers*, Technical Report, Michigan State University, MSU-CSE-15-7, April 2015

2 *Study on Fingerprint Recognition for Children,* Final Report, European Commission Joint Research Centre, Institute for the Protection and Security of the Citizen, Digital Citizen Security Unit, September 2013

3 *Fingerprint Recognition of Young Children*, Technical Report, Michigan State University, MSU-CSE-16-5, September 2016

other forms of biometric identification.[4] 57.72% of respondents reported that they are very comfortable with fingerprint scans – a 17.3% margin over any other approach included in the survey.

These results also hold when considering biometric identification for children under 18. 56% of respondents stated that they are comfortable or somewhat comfortable using biometric fingerprint scans for identity management with minors, a majority saying that they are not very comfortable or not comfortable at all with other modalities. Fingerprint scanning, therefore, represents the most acceptable biometric identity option for children.

Children Are Not Adults

Fingerprint scanner size and resolution are only two of many factors that affect image quality. The emotional and physical immaturity of children introduces other variables that degrade results, including:

- Excessively dry or humid fingers
- Dirty fingers
- Distortion due to excessive, insufficient, or uneven force from the finger on the scanning surface

The JRC testing evaluated three different types of fingerprint scanners to see how off-the-shelf sensor technologies handled image quality under conditions typical with children. The technologies tested included glass optical, multispectral, and touchless (though touchless requires part of a finger be placed in a guide apparatus).

[4] *Consumer Attitudes About Biometric Authentication: A UT CID Report,* Rachel L. German and K. Suzanne Barber, Center for Identity, University of Texas at Austin, May 2018

The project simulated juvenile fingerprint scans under four conditions:

Best – Optimal images generated through multiple scans of dry, clean fingers (goal of NFIQ=1)[5]

Humid – Simulated wet fingerprints (such as a child sucking a thumb) using hand lotion so that differentiating fingerprint features became significantly blurred

Sugar – Moistened fingers inserted into a sugar solution, then allowed to dry, leaving a residue that obscured fingerprint features

Dirt – Simulated dirty or dry fingers created by dipping fingers in granular ash and removing loose particles with facial tissue

These four options generated great variance in image quality. In short, children being normal children, either due to fingerprint condition or a lack of patience with proper positioning requirements, present a significant challenge for generating usable results, and different types of fingerprint scanners compensate for these issues with varying degrees of success.

Other Factors that Impact Image Quality

Environmental factors that affect the scanning sensor itself, such as direct sunlight, bright lights, or temperature extremes, also may lead to poor results. These ambient conditions are relatively simple to control inside a building. However, children in developing countries often live and travel far from these facilities. Rural areas in the Western world face similar challenges.

Governmental, medical, or non-governmental organization (NGO) services cannot be applied if agents cannot reach the target audience. Biometric fingerprint scanners used to verify identity in the field must resist high or low temperatures, residual fingerprints on the sensor surface, bright sunlight, and dirty or damaged fingers, all of which can degrade scanner performance. The units used in the JRC study all struggle with these conditions.

[5] NIST Fingerprint Image Quality (NFIQ) algorithm, which the United States National Institute of Standards and Technology (NIST) designed to predict the performance of fingerprint minutiae matchers. In general terms, NFIQ provides a reasonable indicator of the quality of the image used for enrollment and verification.

Cost is another factor. Multispectral and touchless units cost more than less exotic systems. Government agencies and NGOs operate with limited budgets. High performance is no bargain if the purchaser cannot afford a sufficient number of scanners to meet program goals.

The three technologies tested by the JRC were desktop units. Each is physically fragile. All require heavy, bulky battery packs (commonly called “jump kits”) for field use. These limitations are especially significant when mobile identity management is of paramount importance.

The Ideal Fingerprint Scanner for Children

The ideal fingerprint scanner for accurate enrollment and verification of children must have the following characteristics:

- High-quality images for dry, humid, and dirty juvenile fingers
- Rugged, compact design for mobile as well as desktop operations
- Low power consumption (operates off a smartphone without a separate battery pack)

- Built-in resilience against temperature extremes, bright lights, and direct sunlight
- Affordable and easy to use, without requiring disposable silicone pads or containing internal parts that need replacement

In addition, **the scanner should have a curved surface area to help compensate for poor positioning** for single-finger applications.

Light-emitting sensor (LES) film technology provides another essential element for accurate, reliable imaging of children as young as 18 months. LES-based sensors connect the bezel, the finger, and the platen to create a circuit through phosphors embedded in a thin film substrate. Activated phosphors luminesce to generate a high-resolution image, which is then captured by a CMOS or TFT camera. This arrangement simplifies proper finger placement and the connection between the finger, and the surface significantly reduces opportunities for fraud.

LES scanners are highly tolerant of humid or dry fingers, dirty fingers, temperature extremes, and direct sunlight. There's no need to clean the imaging surface between scans, nor are there membranes or light sources to replace. In short, **LES scanners meet the demands of high-quality imaging for juvenile fingers as young as 18 months.**

Another LES sensor advantage is that the same technology that drives market-leading FBI certified scanners delivers the same quality results for curved sensors. Operators and children often find these curved surfaces to be easier to use and to provide accurate imaging without requiring multiple attempts. The only operational difference between these curved devices and FBI certified products is the curve — FBI standards require a flat surface.

Why Child-Based Identity Management is Essential

Recent research shows that biometric fingerprinting for children is an immediate, practical solution for identity management for individuals as young as 18 months of age. However, the choice of fingerprint scanner significantly affects image quality and the reliability of enrollment and verification operations. These issues are particularly acute for mobile operations, as well as services delivery in the developing world and rural areas within more industrialized nations.

Effective identity management for children using fingerprint scanners requires sensors that operate reliably under potentially extreme field conditions, as well as deliver high-resolution scanning for maximum image quality. These units need to be easy to use, easy to maintain, and affordable. **Overall, curved scanners using LES technology provide the best balance between cost, accuracy, portability, and reliability.**

About Integrated Biometrics

Integrated Biometrics, LLC designs and manufactures FBI-certified fingerprint sensors. The company's patented light-emitting sensor (LES) technology enables lightweight scanners that outperform traditional prism-based devices in size, power consumption, portability, and reliability. Law enforcement, military, homeland security, national identity, election validation, and social services organizations around the world rely on Integrated Biometrics' products to enroll and verify identity quickly and accurately, even in remote locations under extreme conditions. Commercial enterprises and financial services organizations depend on Integrated Biometrics technology to build innovative, highly secure applications to establish and enforce customer identity, in accordance with national and international standards.

For more information, contact Integrated Biometrics:

+1 888 840-8034 | sales@integratedbiometrics.com | www.integratedbiometrics.com