DFS Lab Biometrics Challenge: Measuring fingerprint through android camera

The opportunity

People need to be able to identify themselves to obtain access to needed financial products, government benefit programs, healthcare, and other services. Access to these services can be most beneficial for low income people, however they are ones who most often lack valid identity documents – especially in developing countries. Further, the lack of dependable ID infrastructure creates an opening for fraudulent financial activities, money laundering, and the diversion of government resources.

New approaches to digital identity are rapidly becoming common place – chief among them biometric technologies. Advances in biometric identification in recent years allow for the rapid, secure, convenient identification of individuals using their biometric readings.

The current trend in many developing countries to deploy biometrically enabled digital identity infrastructure also represents an opportunity. Examples include Aadhaar UID in India, NADRA in Pakistan, Biometric voter registration in Tanzania and others in Nigeria, Kenya, Bangladesh, Zambia, and many more.[1] For most of these programs, digital ID infrastructure is put in place and populations are registered *en masse* often reaching most or all of the population as local policy makers attempt to "leap frog" paper and card based ID systems.

However, biometric approaches typically require widespread use of costly biometric readers which can be challenging to deploy and maintain in low resource environments.

Basic phones and even Android smartphones have spread rapidly to many parts of the developing world and may be a solution to this challenge. Our aim is to develop technologies that use standard Android smartphone sensors (i.e. camera) to conduct biometric authentication. The goal is to facilitate a very low cost and easy to deploy digital solution that can be accessed over mobile, downloaded as an app, or integrated into existing apps.

The challenge

*The first challenge launched by the **DFS Tech Biometrics Initiative** is an RFP seeking technologies which are purely software based and can capture and verify fingerprints using only the sensors (i.e. camera) on an unmodified smartphone.*

Development of technology to do fingerprint verification over unmodified Android smartphone (i.e. without requiring any physical peripherals or phone hardware modifications) would allow fingerprint verification to be deployed instantly, anywhere, and zero marginal cost. This could greatly increase access to ID services by removing the need to deploy hardware reader peripherals or buy new biometrically enabled phones.

Primary use cases for this technology include:

- *Onboarding to financial accounts*: Used to complete Know Your Customer (KYC) requirements and identify applicants who are signing up for financial accounts. Here financial institutions

[1] See Review of National Identity systems, EPAR request 306, University of Washington.

would like to verify that the name and/or ID number given during account sign up processes are valid and belong to the applicant against government sponsored biometric databases and blacklists. Allowing people to demonstrate their ID remotely (e.g. as part of an online sign up procedure) without coming to a physical location or interacting with staff would be ideal.

- *Day to day authentication*: Authenticate to access existing financial accounts to trigger transactions or view account details. This use case can often be achieved with password after the initial biometric verification of identity but some service providers might require the extra security of biometric.
- *Government benefits:* Authenticate to receive government benefits payments or other transfers. This is a special case of the KYC scenario above.
- *Non-financial use cases*: The Digital Financial Services Lab has a mission oriented around financial use cases but new biometrics technology that works over android would have many beneficial applications in poverty programs outside of the finance domain.

Success criteria

The ultimate mission of the DFS Lab is to create solutions with a clear path to scale and go to market. We conceive of the following rough design parameters which will allow any software created by the teams to achieve maximum impact.

Operational criteria:

- Teams should aim to create a set of algorithms, processes, or software which is (for purposes of this challenge) is instantiated in a simple Android app that allows for demo and field testing
- The app would have both the finger print capture and anti-spoof technique together
- The primary matching activity is validation (1:1 matching) and not identification (1:N matching)
- Research teams should seek to capture the print and output standard interoperable templates (e.g. ISO 19794-2&4) that could be submitted for matching to central government databases
- Output of the app should be optimized for one of the national ID systems mentioned in this doc. Aadhar in India and NADRA in Pakistan are good candidates.
- If there is consensus across the teams, DFS Lab may build a shared Android application that would function as a common demo app as a shared resource
- Apps will all be field tested in a field test conducted by DFS Lab or other third party to evaluate and compare the apps efficacy in a common context

Performance criteria for successful solutions include:

- **Prove aliveness so that a photo or video of a finger can't be used (this is a critical criteria)**
- Rapidly verify fingerprint (ideally, less than 10 secs to complete full procedure)
- Work on a wide variety of Android phones, older operating system versions, and cameras
- Allow for self-identification by end user without assistance from service provider staff
- Be robust to collusion by service provider staff and end user to defraud the system
- Mitigate risk of data privacy breach or leak of personally identifiable information
- Mitigate risk of security breach, hack, or tampering with the app
- Imply limited data usage and phone battery usage to have minimal negative impact on end user

- With further development, would be modifiable to meet different standards from different biometric systems in different countries
- It's safe to assume primary use case of 1 to 1 validation using Aadhar number (is this person who they say they are?) rather than 1 to N identification (who is this person?)
- Reliably capture fingerprint from variety of races, skin tones, and ages
- Reliably capture fingerprint from people who do hard manual labor, have scars, etc.

What if we already have a solution that captures fingerprints through a mobile phone camera?

We are happy to accept proposals for further refinement of existing solutions. Possible refinements we would consider include (but not limited to):

- Improving liveness detection and anti-spoofing
- Improving functioning within manual laborers and low income populations specific biometrics capture challenges
- Allowing the technology to work on a broader range of Android devices
- Meeting specification requirements to be certified with national ID systems in priority markets (i.e. in South Asia or Sub-Saharan Africa)

Successful proposals will

- Clearly define the approach and ideas for testing and validation
- Address the needs outlined above
- Address all the solution criteria as posed
- Be applicable in the developing world environment
- Have near term practical applicability
- Come from teams that are ready to launch research quickly and deliver prototypes fit for field testing within ~6 months
- Come from teams who would be ready to iterate on the design after field testing
- Propose possible long run go-to-market pathways including IP agreements or launching a startup to drive the technology to scale (for existing commercial players, please define how you plan to integrate the technology into your existing product line)

We will not fund

- Ideas that do not address one of the key challenges described in this call;
- Ideas without a clearly-articulated and testable hypothesis;
- Ideas not directly relevant to developing countries.
- Ideas for which a relevant indicator of success cannot be demonstrated within the scope of the award ($75,000 over 6-8 months);
- Approaches that represent incremental improvements to conventional solutions
- Basic research without clear relevance to the goals of this topic;
- Approaches that present unacceptable safety or privacy risks to individuals (e.g., do not protect personally identifiable information or open avenues for fraud);

Process and timeline:

Our goal is to source innovative approaches to the above challenges which have the potential to eventually scale up to solve the problem at national or global level.

We envision a multistage process as follows:

Initial applications (2 months)

We plan to seek applications from a wide variety of sources, from academia to startups. There is a short online application for initial screening which will lead to phone calls to further explore collaboration with teams that pass initial screening. DFS Lab will convene a group of expert technologists, policy makers, and market players to assess the applications and give input on the worthiest approaches.

Prototype development phase ($75,000 over 6-9 months)

The best approaches will be eligible for up to $75,000 in initial funding to build a working prototype system or to refine an existing product.

Following this iteration, DFS Labs will facilitate a rigorous set of field tests to measure performance.

Follow on: Scale phase

Following these tests DFS Lab will work with the most promising candidates to develop a go to market plan and seek large-scale follow on funding from the Gates Foundation and other sources.

Application procedures

Initial applications comprise a short online form outlining proposed approach, team background, and prior work.

We will accept applications from teams who already have a working product they would like to enhance as well as teams proposing to design something new. For teams bringing an existing product, please lay out clearly what area of performance (aliveness? capture?) you seek to improve and the approach. We will also accept applications from teams who are seeking to meet the certification requirements for Aadhaar or other government systems.

Grant features:

- Up to $75,000 per application with potential for follow-on for the most promising technologies
- 6-9-month term with final convening to share results Q4 2017 or Q1 2018
- Max 10% overhead charge from Universities (per our funders policies)
- Free access to shared software development resources and testing platform
- Shared project costs for joint field testing of solutions coordinated by DFS Lab
- Deadline for applications: 30th May, 2017

Click here for application

The selection committee will contact shortlisted applicants for follow up phone calls and additional application materials. For more information please contact: jake@cariboudigital.net