The Alan Turing Institute

Technical Briefing

Benchmarking Biometrics for Identity Systems in Developing Countries

January 2023

Authors

Professor Carsten Maple, Turing Fellow, Project Principal Investigator, and Professor of Cyber Systems Engineering with Institute partner University of Warwick

Dr Gregory Epiphaniou, Associate Professor in Security Engineering, University of Warwick

Dr Roberto Leyva, Research Associate, University of Warwick

This Technical Briefing is published by The Alan Turing Institute's Trustworthy Digital Infrastructure for Identity Systems project.

This work was supported, in whole or in part, by the Bill & Melinda Gates Foundation [INV-001309]. Under the grant conditions of the Foundation, a Creative Commons Attribution 4.0 Generic License has already been assigned to the Author Accepted Manuscript.

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. It was established in 2015 by five founding universities and became the United Kingdom's (UK) National Institute for Data Science and Artificial Intelligence. Today, the Institute brings together academics from 13 of the UK's leading universities and hosts visiting fellows and researchers from many international centres of academic excellence. The Institute also liaises with public bodies and is supported by collaborations with major organisations.

The Alan Turing Institute
British Library
96 Euston Road
London
NW1 2DB

Table of Contents

1 Purpose

As the United Kingdom's national institute for data science and artificial intelligence, The Alan Turing Institute is driving research into how digital identity systems are evolving to underpin a changing world, including their impact on people and communities, to elevate the requirements for assuring trustworthy outcomes. Biometric technologies are being embraced by lower income and developing economy countries to improve the efficiency of identification services and authentication of claims to public services and resources. This technical briefing gives an overview of various biometric systems their characteristics, applications, limitations, and strengths, examining the appropriateness of varied modalities for lower income and developing economies. It is part of a body of resources and guidance developed in consultation with governments, humanitarian organisations and the industry stakeholders that are advancing digital identity systems.

2 Executive Summary

The cost of a new biometric system is lower than the traditional document-based identity system. Many lower income and developing countries increasingly rely on biometrics as they adopt digital identification technologies, most commonly face, fingerprints, and iris recognition. These solutions are being incorporated into efforts to modernise the legal recognition of identity and public services and often ensure the inclusion of thus far undocumented segments of their population: The absence of a modern identity system is not just an issue of governance but also an economic development issue as digital and online technologies become part of the fabric of society in all corners of the world, and across all economic settings.

Here we review the varied biometric modalities that are being deployed within digital systems. We then present a list of characteristics for assessing their efficacy in achieving their purpose with trustworthy outcomes, for example to deliver consistent and accurate results that are accepted by the society they serve. We also offer a brief overview of the use of biometric technologies in developing countries highlighting considerations relevant to the characteristics and an assessment of the appropriateness of each biometric modality for this setting.

The analysis provides an opportunity to contextually assess the requirements and trade-offs of a given scenario, for example whether cost and accessibility are leading considerations, or whether the system is deployed for a low or high-security environment. Face Recognition systems, for example are widely used in many scenarios, but low performance suggests these systems should only be used combined with human inspection or other biometric systems to ensure security at important places. Further, the high-cost of several systems did not deliver better outcomes according to the characteristic set than lower-cost alternatives.

3 Biometrics in Identity systems

Identities include both static and mutable information about individuals. Identity fields can include name, home address, familial relationship, date of birth, sex, nationality, and biometric information. Identities are extended to cover digital information, for example, an individual account on social media such as Facebook or Twitter. Here we focus on the biometric information. Biometrics provide uniquely identifying information of individuals. A biometric system examines and stores this unique information, facilitating comparison with the individual to validate an identity and in some cases to authenticate access to services and resources. The modern biometric system usually relies on the [1] face, retina iris, fingerprint, hand geometry, palmprint, signature, voice, gait, and deoxyribonucleic acid. Due to the accuracy and accessibility, the face, fingerprint, iris, and signature are commonly used to facilitate enrolment in the biometric system. In addition to underpinning public and commercial services, such systems are used for enforcing criminal and immigration law, national security, and preventing fraud. In this context, fingerprint scans of ten fingers when available for individuals is one of the most publicised biometric techniques [3]. Face recognition extracts facial features from the acquired images and compares the feature distance with the user face images [4]. Iris recognition is an individual feature extracted from human eyes [5]. Similar to iris, retinal recognition requires extracting a feature from the eyes, however the process requires scanning the blood vessels' patterns produced by the capillaries [35].

The biometric system consists of two stages that involve the citizen: (1) enrolment and (2) authentication. For enrolment people provide their biometric which is stored for authentication. In some systems, they store the original copy of biometrics and encoded data or a template interpreting the biometric may be created to enable quick processing in the authentication stage. For authentication, there are two different cases: identification and verification. The identification answers the question 'who are you?'. To find a match, the provided biometric sample will compare with all samples stored in the systems as 1:N (one-to-many) matching. The verification answers the question 'are you who you claim to be?'. The system compares the provided biometric sample with the stored sample of the claimed identity as 1:1 (one-to-one) matching.

Different biometric systems vary in complexity, cost, capabilities, and performance, but they share several essential elements. All biometric systems capture biometrics that can be captured in public and are not sensitive to exploitation. These systems use sensors such as cameras or scanning devices to capture images, recordings, or measurements of human beings. They also rely on computing hardware and software to extract, encode, store and compare these biometrics. Due to the automation process, most biometric systems make decisions very fast, even in real-time. All have some common advantages and disadvantages. They can reduce operational costs associated with operating time or human labour costs. They can improve security due to the high-dimensional features extracted from biometrics. However, these systems are not always 100% accurate. They require integration with sensors which can introduce vulnerabilities. The environment and usage can affect the measurements.

4 Biometric Systems

In this section we provide an overview of some of the most widely used biometric systems, that may be deployed in identity systems in developing nations.

4.1 Facial Recognition System

As the most common and familiar biometric feature, face is widely used in many scenarios. Due to the rapid development of neural networks [6], facial recognition systems are mostly based on the deep learning model. The face model extracts a feature vector from the face image. The system compares the difference between the input vector with the vector extracted from the stored face images. Unfortunately, the deep learning model is still a black box, which means the parameters used for specific decisions are not visible. People recognise faces by facial traits such as nose, mouth, eyes, and the topological structure of these traits. Usually, the face recognition system consists of three parts: Face Detection, Feature Extraction, and Face Recognition. The face detection uses a bounding box technique to determines if the face exists. The feature extraction is the next step to extract the features of the face, identifying local binary patterns or landmarks. The face recognition step makes decisions for verification or identification tasks. The facial recognition system is convenient for users to understand and use. There is no physical contact. Cameras as the sensors are economical to purchase and maintain. However, the facial features will change over a lifetime. Expression, illumination, pose, and occlusion affects the recognition performance. The capture of faces is also sensitive to privacy abuse.

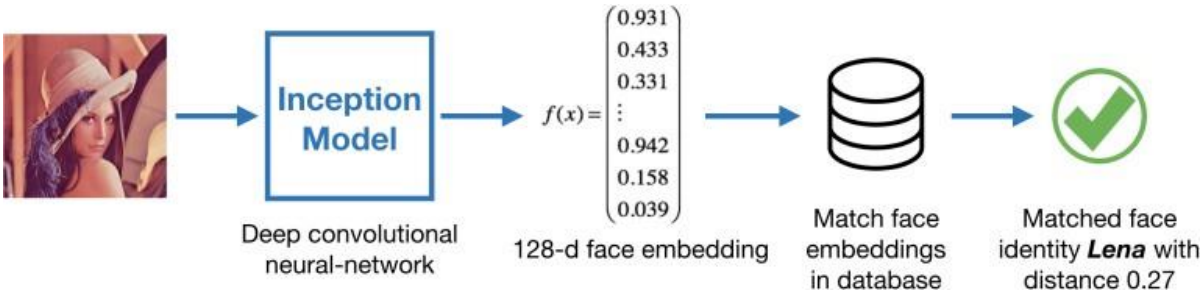

Fig 1: Face Recognition System. Source: [7]

4.2 Iris Recognition System

The iris is a circular colour piece of the human eye. The iris is unique for everyone, even for identical twins, while also being a constant through life [8]. For the same individual, the left and the right irises have different patterns. The iris cannot be changed by eye surgery or wearing glasses and contact lenses. Iris images are usually captured by infrared light. The iris recognition system works with infrared light regardless of eye colour [9]. Therefore, the iris recognition system offers a promising accurate rate. Due to the size of the eyes, the sample size is small. The iris recognition system has a low cost of storage. The sensor is a camera which means there is no physical contact with the system. Most iris recognition systems are based on machine learning methods that are explainable and tractable. However, the iris recognition system has some

disadvantages. Due to the relatively small market, the cost of the system is comparatively high. The scanning requires the users' cooperation. Iris is not changed by eye surgery or wearing glasses and contact lenses but can be obscured. Illumination should not be visible or bright since users stare at the sensor. The sensor is sensitive to distance, if the distance is too far the algorithm cannot extract patterns from the relatively small samples. Also, the algorithm is sensitive to image quality. Some severe diseases such as diabetes may change the iris patterns. Iris capture has disadvantages including physical difficulty in acquisition, e.g. the length of time to acquire multiple images and the discomfort this may cause. The perception of intrusion and potential physical damage to the eye can also limit acceptance and application of the technology.

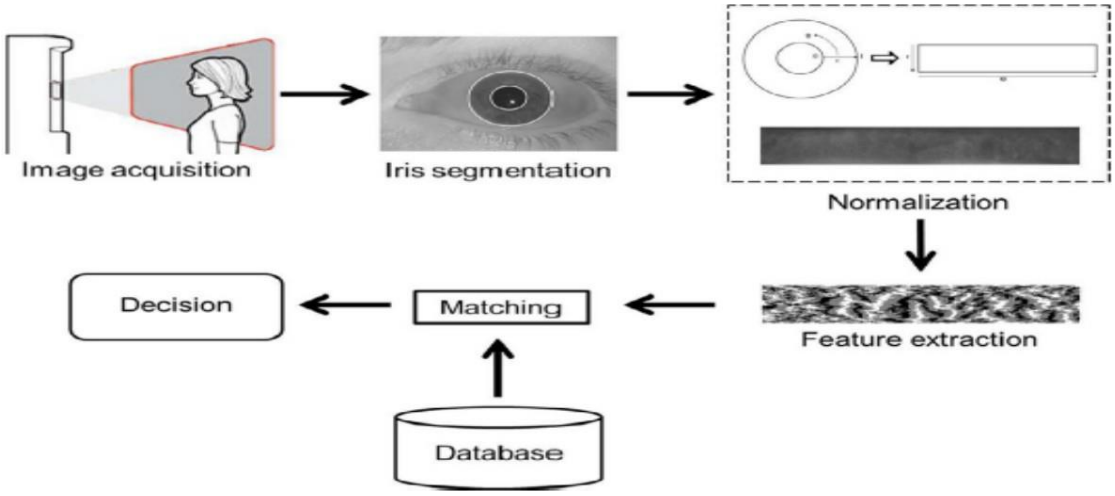

Fig 2: *Iris recognition system Source:* [10]

4.3 Retinal Recognition System

The retina is a light-sensitive tissue where light is transformed into nerve pulses sent to the visual cortex to capture images. The blood vessels in the tissue create unique patterns among people. As these patterns are not genetically determined, they are deemed to be unique [1]. Like Iris, commonly this human feature changes little during a lifetime and is difficult to alter [36]. Retinal features are exceptionally reliable. Even identical twins produce different patterns. There is no need for physical contact to extract them, and it requires user consent to produce them. Further, damaging the retina is more difficult than with other biometric sources, e.g., fingerprints. Nevertheless, this biometric presents disadvantages. There is misconception around the risks of permanent damage, which has fuelled negative opinions about the technology. Retinal features require adequate illumination environment whether it be indoors or outdoors. The technology is considered friendly as the user needs to be close to the capturing device and in certain positions, while eyewear, such as eyeglasses, may make the acquisition difficult. Some medical conditions create challenges, e.g. people with astigmatism may not produce reliable features. Compared with other technology, e.g., fingerprint, retinal biometric is significantly more costly [36]. The process for retinal biometrics is just like Iris, differing from the feature's source only.

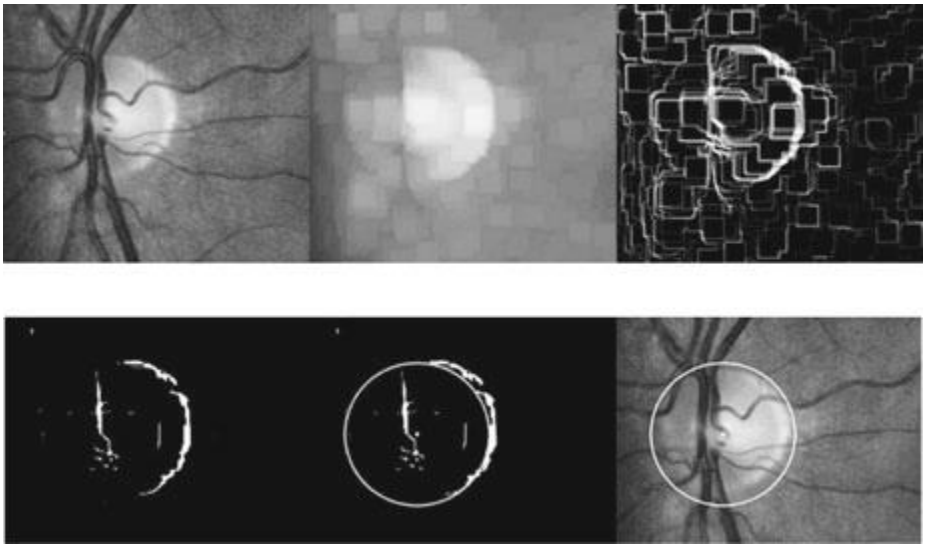

Fig 3: *Retinal feature extraction, the scan (upper left) requires an image processing pipeline to detect the Hough circle (lower right) from which the feature is extracted. The process requires blurring, first order filters, edge detection and binarization to locate the feature's location area. Source:* [36]

1

4.4 Hand-based Recognition Systems

There are many different systems that are based on features of, on, or within the hand. We discuss some of the most common and applicable hand-based biometric systems.

4.4.1 Fingerprint Recognition System

The fingerprint is the texture pattern of interweaved ridges and valleys present on the surface of the finger [11]. Due to the physical difference between the ridges and valleys, the ancient ink-and-paper system was used for fingerprint recognition thousands of years ago. The ink-and-paper system uses ink to record the peaks of friction ridges on the skin to a smooth surface such as paper. Modern fingerprint recognition systems replicate this technique using more sophisticated tools. The ridge patterns are different among different fingers, even for identical twins or the same person. The ridge pattern does not change during the lifetime. However, some people do not have ridges and valleys. Some diseases may change the ridge patterns [12]. The system, therefore, is highly secure and reliable when all ten fingerprints are used as samples. The sample size is small which has an impact on storage costs. The market for fingerprint systems is mature and the technique is widely used. The system can choose different numbers of fingerprints to balance between the cost and security. However, the fingerprint system can be attacked by artificial fingerprints made of wax, for example, while any cuts, scars, or absence of users' fingers can lead to misidentification. The users have physical contact with the system. Dirt and twists can easily distort the system.

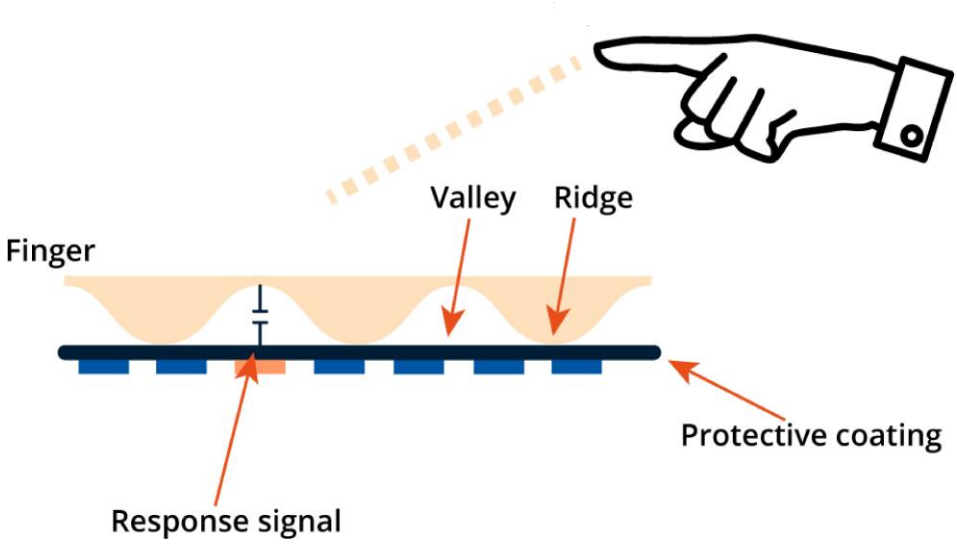

Fig 3: *Iris recognition system capacitive sensing Source: [13]*

4.4.2 Hand Geometry Recognition System

Unlike the fingerprint, hand geometry consists of finger length, finger width, finger thickness, finger area, and palm width. These features are not stable until later life. Illness and weight affect these features. These features are not sensitive to the environment, such as dirt on the hand or any cuts or scars. The system can accept low-quality images because it does not focus on the details such as texture or ridges. Therefore, the cost of computation and storage is relatively low.

4.4.3 Palmprint Recognition System

The palmprint is a record of the palm region consisting of principal lines, epidermal ridges, and minutiae points. The palmprint is unique for individuals. As a subcategory of the hand-based recognition systems, the palmprint shares similar advantages and shortcomings with the fingerprint. However, the palmprint recognition cost is higher due to the larger size of data.

4.4.4 Palmvein/Fingervein Recognition Systems

The vein recognition system is a new biometric technology proposed in recent years [16]. The vein is unique to individual; however, it requires high-resolution images for vein pattern recognition. The cost is relatively high, while the performance is not satisfactory. The veins are highly stable, robust, and developed before birth, but the pattern can be easily affected by body temperature and heat.

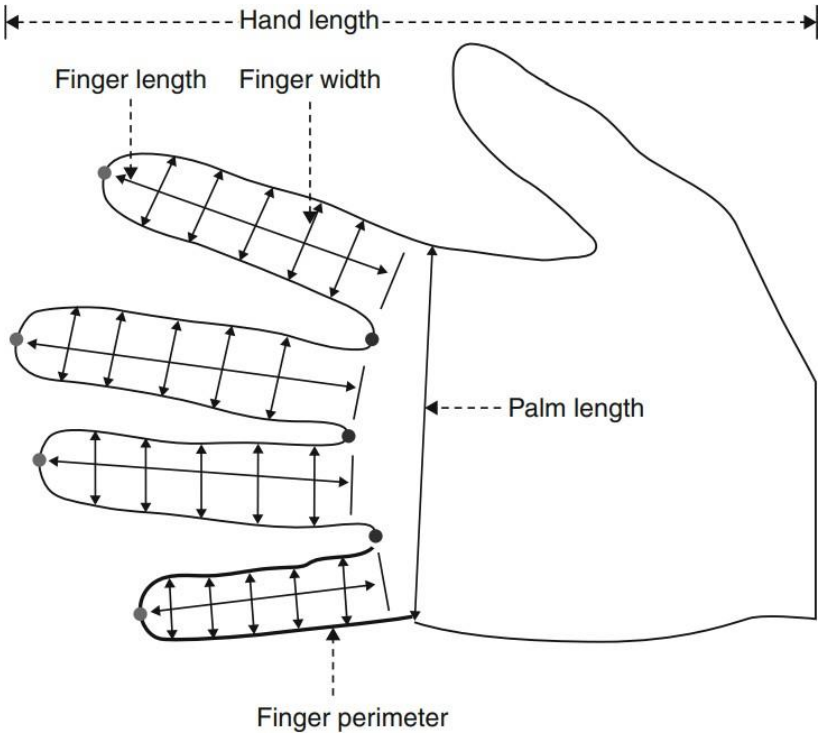

Fig 4: *Hand Geometry Source:* [14]

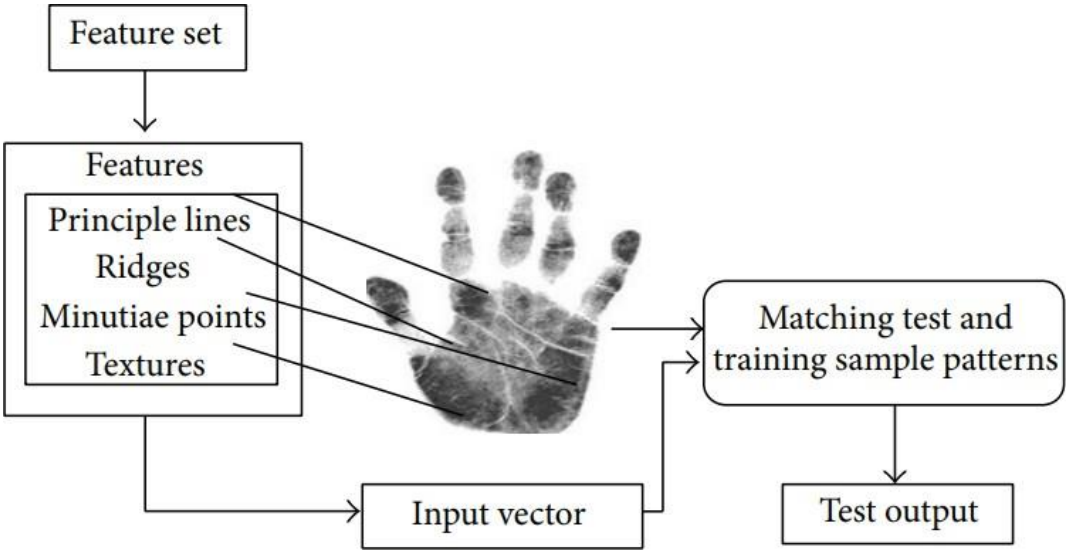

Fig 5: *Palmprint Source:* [15]

4.5 Voice Recognition System

An individual's voice is determined by their physical attributes such as vocal tracts, mouth, nasal cavities, and lips. Voice biometrics involve four primary steps. (1) Capturing voice and converting to a digital signal. (2) Converting the digital signal to a voiceprint with distinct sound characteristics. (3) Creating and storing a model as a template that uniquely identifies speakers. (4) Validating the voice with the template. It is an automated and non-contact process. If the speaker's attribute matches with the template, the system will return as a match, or a no-match is given if no templates matching their attributes are found. [17] [18]

There are two types of voice recognition techniques, Automatic Speaker Verification (ASV) and Automatic Speaker Identification (ASI). ASV is used in a two-factor authentication scenario, and ASI tries to determine the speaker's identity. Since most personal devices come with a microphone, it is economical. It is widely used in the banking sector for validating speakers remotely in a call. Voice might sometimes vary due to the individual's medical condition, age, or circumstances.

Voice biometrics in developing countries has very high potential, due to the penetration of mobile phones (Feature phones as well as smart phones). The use of voice coupled with an interactive voice response system enables authentication and access services.

4.6 Gait Recognition System

By focusing on an individual's body shape and the unique way that the body moves when walking or running, it is possible to identify a person over a long distance without direct contact. A gait is a person's walking pattern, and gait recognition means authenticating a person by the way they walk. In surveillance applications, it is often difficult to get precise information about the iris or face due to a low video resolution. This shortcoming made gait analysis gain popularity in recent years. Several medical and psychological studies have shown that there are 24 different components to human gait [19,20], these components represent a gait "signature" that can be linked to a person's identity.

Gait Recognition Systems (GRS) combine computer vision techniques and machine learning technologies to recognise a person's gait using data collected from several sources (video camera, motion sensors, etc.). The collected data goes through several processes such as silhouette segmentation and contour detection to extract gait features that will be used for person identification. GRSs have several advantages to other biometric systems: First, gait features are hard to imitate because it relies on human silhouettes and activities. Second, gait recognition can be done from a distance without close human intervention and even the individual's cooperation. Finally, they can work well on low quality videos/images and when face or iris features are hidden [21]. One major drawback, however, is the need for high-quality datasets which can only be constructed with special sensing panels and a high-resolution camera, collected in controlled environments, which makes scaling such solutions problematic.

4.7 Signature Recognition System

Signature Recognition is another form of behavioural biometrics that can be used to identify a person based on their handwriting. The system observes the trace of pen on paper and analyses its shape along with certain features and measurements to identify or verify the identity of the writer. Signature recognition can be done using two modes:

1. Static mode or “off-line” mode: The user first starts by writing their unique signature on paper, the paper is then scanned through an optical scanner or a camera to transform the image of the signature into bits. The system analyses the shape of the signature as well as 40 other characteristics including centre of gravity, edges, and curves for authentication.

2. Dynamic mode or “on-line” mode: Instead of signing on a paper, users write their signatures directly on a digitalising tablet which captures data in real-time. The main difference between this and an offline mode is that the system in this mode captures more accurate information such as x,y coordinates, pressure, time and pen velocity which provide a high level of accuracy for the signature verification.

Since these systems focus more on the behavioural pattern of signatures, they are quite resistant to impostors: It can be easy to forge an actual signature, but imitating these patterns is quite difficult. Another advantage is that these technologies are considered non-invasive and user-friendly. There is a high probability that they will be accepted by users as an authentication mechanism. The main drawback is that when the behavioural characteristics of signatories are mutually inconsistent with each other, signature recognition systems are subject to much higher error rates.

4.8 Deoxyribonucleic Acid Recognition System

Deoxyribonucleic acid (DNA) is presumably the most reliable biometric modality widely used in forensics and healthcare. DNA can be acquired from the body fluid, nail, hair, and it is unique for everyone, except for identical twins. A buccal swab is the most convenient and easy way to collect DNA from epithelial cells; it involves wiping a small cotton swab in an individual’s cheek. Later the swab is dried and transferred to storage space. [22] DNA biometrics involve measuring short tandem repeat sequences (STRs) in the nuclear or mitochondrial DNA. Before the emergence of rapid DNA identification technology, it wasn’t easy to get the length of the STRs in DNA. It took multiple types of equipment, specific labs to perform the task, and many days to get the result. Rapid DNA identification technology contains portable desktop equipment with a processing time of around 90 minutes.

DNA biometric systems are different from others in multiple ways, (1) They compare the actual sample instead of using templates or feature extraction. (2) DNA needs an actual physical sample unlike fingerprint, face, or voice. (3) DNA matching is not real-time. The contamination of the sample can impact the accuracy. DNA contains a lot of information about the individual, which can be used against the individual, which introduces high risk considerations for storing the samples and data securely. [23]

5 Characteristics for measuring the efficacy of Biometric Systems

Before deploying any biometric measurement into an identity system, an assessment needs to be made regarding the suitability of the biometric. To provide inclusivity, for example, it must be the case that every person has that biometric. This characteristic is usually termed *universality* in the analysis of biometrics. There are a number of characteristics that can be used to describe the suitability of metrics, including recommendations by the US National Institute of Standards and Technology (NIST), as well as proposals by academics [24–27]. In analysing these resources, the measures we deemed appropriate for assessing the biometric for use in identity systems in developing countries are:

- Universality: the biometric should be possessed by every person
- Uniqueness: the biometric should suitably distinguish any two individuals
- Permanence: the biometric should not be drastically affected by age or use
- Collectability: the biometric should be easily acquired through non-invasive means
- Acceptability: the biometric should be approved for widespread public use
- Performance: the biometric should be reliable in identifying individuals
- Circumvention: the biometric should not allow adversaries to easily bypass it
- Capacity: a large number of samples of the biometric should be able to be stored in the system
- Mobility: a biometric record should be able to be transferred to other places easily
- Interference: the biometric should not be affected by the presence of physical or electromagnetic impediments
- Invasiveness: collecting the biometric should not introduce user discomfort
- Cost: the cost of developing the system (including recording, storing and verifying) and utilising the biometric should not be prohibitive
- Speed: the biometric should verify or identify an individual in a suitable timeframe
- Stability: the system should perform equally well under different environments
- Popularity: the biometric should have a mature market including the manufacturer of hardware and the service provider of software

6 Biometric Systems in Developing Countries

6.1 Overview

It takes centuries to develop and mature an identity system in developed countries [28]. In developing countries, the traditional identity system is often not as sophisticated as in developed countries. Many developing countries, for example, lack official documentation of birth. [29]. Without an official birth certificate, citizens can be treated as if they do not exist: They suffer from a lack of access to public services, an inability to open a bank account or travel, and other disadvantages. Recently, many developing countries have embraced biometric-based identity systems to address this, alongside other governance, and development policies.

As a result, unlike in the most developed economies, the biometrics market did not originate from law enforcement or border control, but from the broader requirements of service delivery, which has had an impact on the pace of implementation and characteristics of the biometric systems themselves. *The Africa and Middle East biometrics market is forecast to grow at an annual rate of* 21%*, with the global biometrics industry set to reach US $82 billion dollars by 2027* [30]. Fingerprint and face recognition are the two most popular methods. A sufficient biometric system benefits not only the development but also the broader investment being made in identity schemes [31]. *"A number of biometric registration laws are too complicated and not adapted to the modern world. In some cases, people have to produce physical documents as opposed to electronic versions,"* says Dr Joseph Atick, the executive chairman of Identity for All in Africa (ID4Africa), an NGO that works with African countries to establish identity ecosystems. Aadhaar, India's ambitious Universal ID programme is the largest biometric identification program in the world. The Unique Identification Authority of India (UIDAI), which collects iris scans of both eyes, ten fingerprints, and a digital face image from each enrolee, covers more than 1 billion people and has a target of 1.4 billion as of 2021 [34]. The programme is used as an example for creating a national biometric systems in developing countries. While fingerprints are easier and cheaper to be deployed around the country, the two iris scans facilitate better inclusivity while ensuring better security of the authentication process. Many people, especially the elderly and manual labourers, have worn fingerprints and or damaged eyes. The two methods combined together ensure accessibility for these individuals. Aadhaar protects individual privacy by only returning a verification result of 'yes' or 'no' to a query, rather than the underlying detail, while the standard for accountability, scalability, and technical compliance are transparent. Further, the cost goes down with competition among different service providers. It's cardless design also makes it convenient for application to other purposes, for example, personal banking, in place since 2019. Explainable jurisdiction, therefore, is important for the programme.

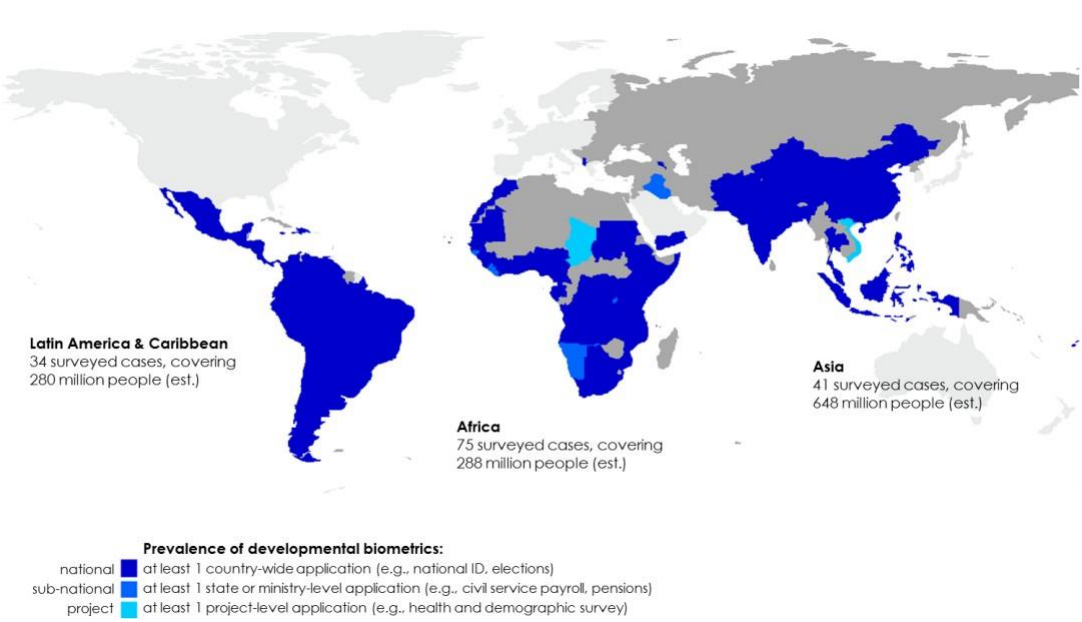

Fig 6: *Survey of the Use of Biometrics Technology for Development, Low-Middle Income Countries (2012) Source:* [33]

6.2 Applicability of biometric systems in developing countries

Table1 provides an evaluation of the applicability of different biometric modalities in identity systems for developing countries. It can be seen that facial recognition systems are suitable for fast, low-cost, low-security environments. However, face recognition performance is low, so it should not be relied upon in isolation as an authentication process. The facial recognition system should be used combined with human inspection or other biometric systems to ensure security at important places, for example. That being said, the facial recognition system is suitable for use in most developing countries, given the relative cost, collectability and acceptability the iris and retina recognition systems share similar traits. Their sensors are not friendly to users, however, and the cost of these systems is high. These two recognition systems are commonly used for high-security, high-cost environments such as bank vaults and confidentiality departments. These two eye-related systems should not be the first choice for developing countries.

Table 1

Comparison of Various biometric techniques based on biometric traits. L- Low, M-Medium, H-High

Traits \ Biometric	Face	Iris	Retina	Fingerprint	Hand Geometry	Palmprint	Hand-vein	Voice	Gait	Signature	DNA
Universality ↑	H	H	H	M	H	M	M	M	H	L	H
Uniqueness ↑	M	H	H	H	M	H	M	M	M	L	H
Permanence ↑	M	H	M	H	L	H	M	L	M	L	H
Collectability ↑	H	H	H	M	H	M	M	M	H	H	L
Acceptability ↑	H	M	L	M	M	M	M	H	M	H	L
Performance ↑	L	H	H	H	M	H	M	L	L	M	H
Circumvention ↓	H	L	L	M	M	M	L	H	M	H	L
Capacity ↓	H	L	L	L	L	L	L	M	H	M	H
Mobility ↑	M	H	H	H	H	H	H	M	M	M	L
Interference ↓	M	H	H	M	H	H	H	M	M	M	L
Invasiveness ↓	M	H	H	H	H	H	H	M	L	L	H
Cost ↓	M	H	H	L	H	H	H	L	M	M	H
Speed ↑	M	M	M	H	H	H	H	H	M	H	L
Stability ↑	L	H	M	L	M	M	H	L	L	L	H
Popularity ↑	H	M	L	H	L	L	L	H	L	H	H

↑ –H > M > L, ↓ –L > M > H

Fingerprint is another popular recognition method to be considered as an appropriate choice for developing countries. The fingerprint is suitable for high-security and low-cost scenarios. The system is also friendly to users and economical for sample storage. They are subject to interference from dust or dirt to users' fingers and should be combined with other modalities to ensure inclusivity in the case of missing or labour-worn fingerprints. It requires contact and has a requirement for hygiene. Compared to fingerprint biometrics, other hand-based recognition systems including hand geometry, palmprint and hand-vein, are not suitable for developing countries due to their high cost. Despite their higher cost, these methods did not outperform the fingerprint biometric system according to other items in the characteristic set. The voice biometric system is similar to the face biometric system. It is suitable for a low-cost and low-security environment. However, due to the low permanence of the voice, this system should be developed on portable devices such as smartphones or computers, which allow users to re-enrol their current voice biometric over time. The gait biometric system has similar traits to face biometric system. Unfortunately, the gait recognition market is not as mature as

the face recognition market. It is not as socially acceptable as face recognition, and the gait recognition requires the user to walk one gait cycle (1-1.3 seconds) [34] requiring more space and time. The signature biometric system is as popular as the face, the fingerprint and the voice ones. The issue of the signature system is the low-universality and low uniqueness which means it is easier to be attacked or to return incorrect decisions. DNA is very popular. DNA is suitable for high-security and high-cost environments. Due to the low collectability, acceptability, mobility, and speed, DNA can be ideal for the authentication process that makes a final decision to identify an individual. However, in developing countries financing laboratories to process the data may not be a feasible solution, because the price is high compared to other biometrics [37].

7 Summary

In this paper we have presented an overview of the major biometric modalities that can be utilised in identity systems at scale in developing countries. We have, through analysis of the extant literature, devised a feature and characteristic set which can be used to evaluate the suitability of these biometrics. Finally, we have analysed each of the biometrics and evaluated their suitability for deployment in developing countries.

This analysis was developed to inform technical choices in the development of trustworthy identity systems, that reflect the requirements for robustness and reliability alongside ethical considerations such as acceptability and other facets suitable for the purpose and context for which they are designed.

8 References

[1]N. K. Ratha, J. H. Connell, and R. M. Bolle, “biological measurements unique to each person, such as finger- prints, hand geometry, facial patterns, retinal patterns, or other characteristics that are used to identify individuals,” *Committee on Technology, Privacy Biometrics: Building a Conceptual Foundation 4 (2006)*, 2006.

[2]“Rfid chips are designed to automatically emit radio waves to transmit stored information to receiving units.” [3]N. Science and T. Council, “Committee on technology, privacy biometrics: Building a conceptual foundation 4,”
2006.

[4]A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in *Advances in Neural Information Processing Systems*, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Wein- berger, Eds. Curran Associates, Inc.

[5]M. J. Burge and K. W. Bowyer, *Handbook of Iris Recognition*. Springer Publishing Company, Incorporated, 2013.

[6]A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet Classification with Deep ConvolutionalNeural Net- works,” in *Conference on Neural Information Processing Systems*, 2012.

[7]C. Zhuge, X. Liu, X. Zhang, S. Gummadi, J. Xiong, and D. Chen, “Face recognition with hybrid efficient convo- lution algorithms on fpgas,” 05 2018, pp. 123–128.

[8]J. Daugman, “How iris recognition works,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[9]D. F. R. J. B. R. J. Roizenblatt R, Schor P, “Iris recognition as a biometric method after cataract surgery.” *Biomed Eng Online*, 2004.
[10]H. Ahmed Salman and M. Taha, 2021.
[11]M. M. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, “Overview of fingerprint recognition system,” in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1334–1338.
[12]K. Harmon, “Can you lose your fingerprints?” *Scientific American*, 2009.
[13]Argustrueid, “Fingerprint identification,” *https://www.argustrueid.com/fingerprint-identification/*, 2004.
[14]D. Zhang and V. Kanhangad, *Hand Geometry Recognition*. Boston, MA: Springer US, 2011, pp. 529–531. [Online]. Available:https://doi.org/10.1007/978-1-4419-5906-5 878
[15]M. Nappi, S. Kanchana, and G. Balakrishnan, “Palm-print pattern matching based on features using rabin-karp for person identification,” in *The Scientific World Journal*, 2015.
[16]J. R. G. Neves and P. L. Correia, “Hand veins recognition system,” in *2014 International Conference on Computer Vision Theory and Applications (VISAPP)*, 2014.
[17]K. Delac and M. Grgic, “A survey of biometric recognition methods,” in *Proceedings. Elmar-2004. 46th Inter- national Symposium on Electronics in Marine*, 2004, pp. 184–193.
[18]F. Abbaas and G. Serpen, “Evaluation of biometric user authentication using an ensemble classifier with face and voice recognition,” 2020.
[19]C. P. Charalambous, *Walking Patterns of Normal Men*. London: Springer London, 2014, pp. 393–395. [Online].
Available:https://doi.org/10.1007/978-1-4471-5451-8 99
[20]M. MP, *GAIT AS A TOTAL PATTERN OF MOVEMENT*. Springer London, 1967, pp. 290–333.
[21]V. V. CHANGSHENG W., Li W., *A Survey on Gait Recognition*. ACM Computing Surveys, 2019, pp. 1–35. [22]M. Hashiyada, *DNA biometrics*, 06 2011.
[23]S. Bhable, S. Kayte, R. Maher, J. Kayte, and C. Kayte, “Dna biometric,” vol. 5, pp. 2319–4200, 11 2015.
[24]L. Siwik and L. Mozgowoj, “Server-side encrypting and digital signature platform with biometric authorization,”
International Journal of Computer Network and Information Security, vol. 7, pp. 1–13, 2015.
[25]V. P. Venkatesan and K. Senthamaraikannan, “A comprehensive survey on various biometric systems,” 2018. [26]SundararajanAditya, I. SarwatArif, and PonsAlexander, “A survey on modality characteristics, performance eval-
uation metrics, and security for traditional and wearable biometric systems,” *ACM Computing Surveys*, 2019. [27]M. El-Abed, C. Charrier, and C. Rosenberger, 11 2012.
[28]E. Higgs, “Identifying the english: a history of personal identification 1500 to the present.” *London: Continuum*, 2005.
[29]“The ’rights’ start to life: A statistical analysis of birth registration.”
[30]F. Toesland, “African countries embracing biometrics, digital ids.” *African Renewal*, 2021. [31]C. Burt, “Biometrics in the developing world.” *Biometric Update*, 2017.
[32]A. Gelb and J. Clark, “Building a biometric national id: Lessons for developing countries from india’s universal id program.” *Center for Global Development Brief October*, 2012.
[33]——, “Identification for development: The biometrics revolution,” *SSRN Electronic Journal*, 2013.
[34] A. Nair et. al. “*Digital Public Services: The Development of Biometric Authentication in India*”, Springer International Publishing, 2023
[35] H, Josef and D. Martin “*Recognition-Based on Eye Biometrics: Iris and Retina*”, Springer International Publishing, 2019
[36] M. Obaidat, I. Traore and I. Woungang “*Biometric-Based Physical and Cybersecurity Systems*”, Springer International Publishing, 2019
[37] Gayathri, M., C. Malathy, and M. Prabhakaran. "*A review on various biometric techniques, its features, methods, security issues and application areas*." International Conference On Computational Vision and Bio Inspired Computing. Springer, Cham, 2020.