Biometric Authentication Review

Horațiu Luci
ULB
horatiu.luci@ulb.be

6 January 2021

Abstract

Information Security is nowadays an entwined field with the one of Information Technology to the point where the line between them is effectively blurred. Authentication plays a big role in the process of ensuring security and more specifically access control. This paper will shed light upon the biometric authentication processes and the future developments. A human being has a number of unique physical characteristics which are the point of interest in biometrics. Essentially, various systems will assess a number of these characteristics using reliable recognition schemes and based on that assessment only a legitimate user will be granted access to the system's rendered services. This work underlines the position of the subfield of biometrics within the field of Cyber-Security, further outlining opinions about these systems, making comparisons highlighting various benefits as well as drawbacks.

1 Introduction

The assurance of information being confidential and its integrity as well as availability in all forms is a matter of information security and a number of techniques can support this task. However, a way that is both extremely convenient due to the recent advancements in technology as well as secure due to the indisputable uniqueness of each individual is biometric authentication. This method is known to to support the facet of authentication, identification and non-repudiation and it has exponentially grown in popularity due to the popularisation of smartphones. However it is a vulnerable technology against identity theft if implemented incorrectly but yet this issue has seen a decreasing amount of concern in the recent years. With our society becoming more and more widely-networked, the use of more classical authentication techniques such as possession-based (using something unique in one's possession such as an access card) and knowledge-based (using a unique piece of knowledge that one has such as a code or password) is becoming increasingly obsolete as the advantage of a biometric system is establishing a 1-to-1 mapping between one person and their afferent piece of data. This paper will develop a detailed dive into biometric authentication techniques, that will provide an insight into this sub-field's past, present and future.

2 Overview

Biometrics (ancient Greek: bios =”life”, metron =”measure”) initially was a reference to the field of “biological statistics”, that is, the quantification, analysis and administration of massive amounts of data on biological communities (e.g: a grass field, a forest)(1)
As technology evolved, it is the reference that we now all know - authentication someone - assessing the claims that one makes they are based on an aggregate of their physical features. The past, present and future developments are studied below:

2.1 Past

The first example of a fingerprint scan can be traced back to the 14th century China, where children fingerprints have been fount to be taken by merchants for the purpose of identification. By the end of 19th century, further studies of the mechanisms of the body have been made in order to help with criminal identification. One consecrated method was the Alphonse Bertillon method which was used even by the authorities until various false positives have been detected. After this, fingerprinting was brought-back as the primary method of identification.(2)
In the 20th century, research progressed further into the field of biometric research and by the end of it, Karl Pearson made important discoveries which would prove important for this field. Some of his work, such as method of moments, the Pearson system of curves, correlation and the chi-squared-test was done through studying statistical history and correlation. Later, up until 1980s biometric authentication procedures based on signature were developed, but the field was mostly focused on fingerprints, with increasing amounts of technology supporting it.

2.2 Present

Biometric authentication is an ever-growing sub-field of Cybersecurity and IT as well as a controversial one due to the concern over identity theft and privacy issues. Laws and regulations concerning this subject are largely established in some parts of the world (such as the General Data Protection Regulations) while in others they are lacking behind. Face recognition and fingerprinting technologies have largely been adopted by most people, however, in the form of smartphones but nevertheless, the technology is still being rapidly-growing. We can see 2 main classes of characteristics for the in the modern approach:

- Physical: related to the body features of one person. (face recognition, vein prints, iris scan)
- Behavioural: related to the behaviour of a person, such as, keystroke dynamics and voice.

Recently, ‘browser-fingerprinting’ has been developed as a technique which aims to match everyone using one website with their social-media presence thus personalising the website differently for every user regardless of their cookies. This is however a more improper way of biometrics and it comes with a lot of privacy concerns.

2.3 Future

A biometric system is tasked with two functions: verification and authentication. These techniques will be required to be stringent enough to employ both of the aforementioned tasks. Cognitive biometrics are developed to asses a user's response to various stimuli (such as olfactory or visual), as well as mental performance and facial expressions scan to be used at high security areas. Many other biometric techniques have recently been or are in the process of being developed, such as: DNA, hand veins, way of walking.

After research, is has been largely determined that the best approaches that will satisfy both the verification and the authentication features will be to scan the iris, finger print or palm veins. However the constrain that comes up is performance in day to day use. For instance, for iris scanning, after detection of the general iris pattern, the distance between the iris-boundary and the pupil can be calculated. This feature is used for the recognition tasks, since it's a unique feature for everyone. However, in a real life application of this problem it has been observed that the target value fluctuates and it may need to be updated as time passes on. This is a recent development which is in turn aided by the evolution in the field of Artificial Intelligence.

3 Applications

A defining feature of the biometric authentication is its high reliability. Since human features compared to passwords or PINs are much more difficult to forge, recent advancements in computer hardware made way for instant authentication with face recognition or even iris scanning which provide instant access to resources, transactions, data, application login and much more with fast processing sensors and memory. This is a significant development that took place in the last 10 years due to the recent trend of technology to become more portable.

More applications include: financial transactions, electronic banking, health services, law enforcement, shops, etc. This technology already plays a big role in personal authentication all across the world wide web. The fact that it can be used and integrated with other security technologies such as access cards, will make biometrics prevail as the only way to authenticate a person.

4 Evaluation

The degree of security as well as convenience are the most important factors when using biometric authentication in a real-life situation. We have discussed the history and practical aspects of the technique and in this more technical section, we will evaluate the security of these systems from a technical standpoint based on multiple assessment factors which have proven to be effective in quantifying the degree of security and convenience in a real-life situation. (3; 4; 5)

4.1 Factors of Evaluation

4.1.1 False Accept Rate (FAR) or False Match Rate (MAR)

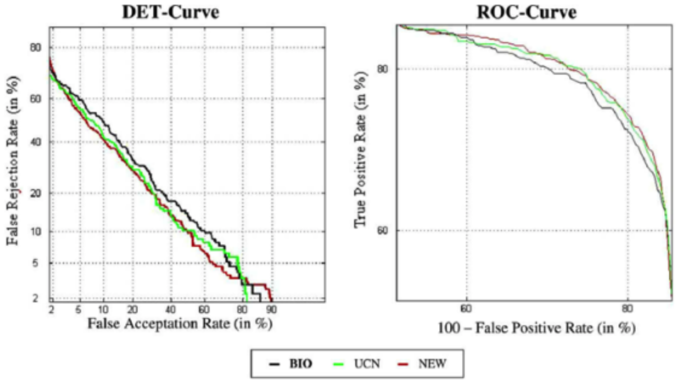
Probability with which the system will successfully match the input pattern and a non-matching pattern that has previously been stored. This system is critical in assertion of granting or forbidding an access and this measurement indicates the percent of invalid matches.

4.1.2 False Reject Rate (FRR) or False Non-Match Rate (FNMR)

Probability with which the system incorrectly fails to match the input pattern and one of the saved template patterns. The percent of valid inputs being rejected is not as important as the previous metric considering that a user can retry to authenticate instantly or after some time.

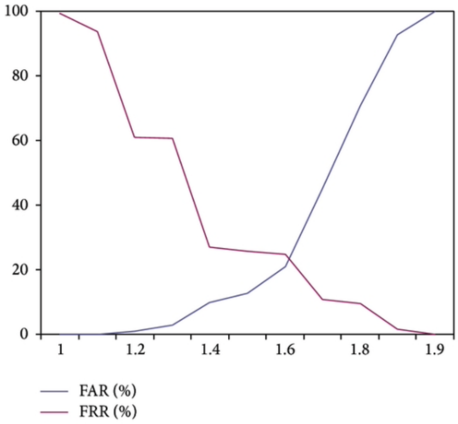
4.1.3 Relative Operating Characteristic (ROC)

The matching algorithm generally performs the decision using a set of thresholds. The FRR and FAR are usually traded-off one agains another by changing the thresholds for which they accept or deny a particular user. The ROC can be plotted by plotting the intersection between the values of FAR and FRR as the thresholds are increasing or decreasing. Another common variation on the same theme is the Detection Error Tradeoff, obtained by deviate normal scales on both axes, and as shown, it is a more easy to tell the difference in performance.



4.1.4 Equal Error Rate (EER)

The point at which FRR and FAR are equal. ROC or DET plotting helps showing how the accept and reject rates can be changed. ERR is generally used as the need of comparison between two systems needs to happen fast. So because of how FRR and FAR can be change, the lower point at which they are equal is, the more accurate the biometric system is regarded as.



4.1.5 Failure to Enroll Rate (FTE or FER)

The rate at which data input is considered not valid and fails to even register into the system. This usually happens due to low quality of the sensor as well as an incomplete scan.

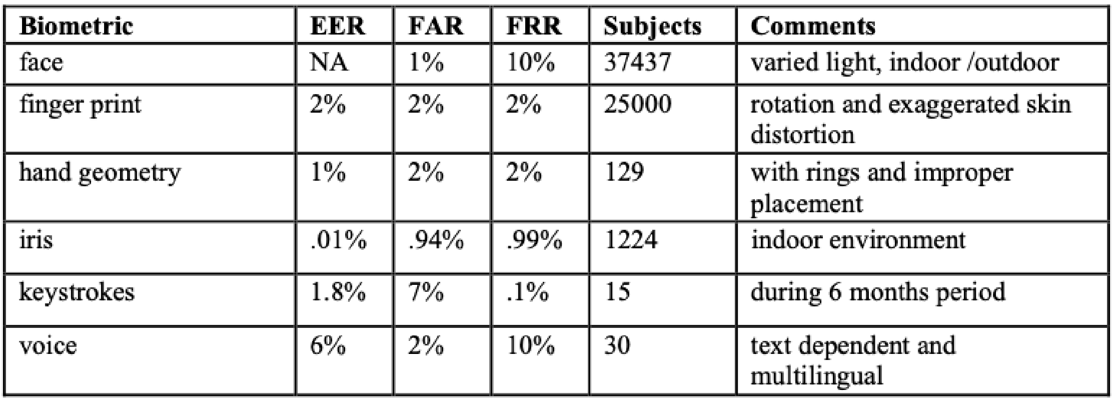
4.1.6 Failure to Capture Rate (FTC)

The rate at which a system will fail to detect a biometric characteristic even though it has been correctly presented.

4.1.7 Template Capacity

Defined to be the number of templates that a biometric system can store to check against. Usually it is desirable to have an unlimited number of templates. However due to the nature of the data, currently it's limited to less than ten for consumer systems.

Evaluation of some techniques



Biometric	EER	FAR	FRR	Subjects	Comments
face	NA	1%	10%	37437	varied light, indoor /outdoor
finger print	2%	2%	2%	25000	rotation and exaggerated skin distortion
hand geometry	1%	2%	2%	129	with rings and improper placement
iris	.01%	.94%	.99%	1224	indoor environment
keystrokes	1.8%	7%	.1%	15	during 6 months period
voice	6%	2%	10%	30	text dependent and multilingual

5 Details and Evaluation of Techniques and Technologies

As previously mentioned, there are two types of biometric characteristics and so the techniques existent are based on them. Details of each characteristic, with a special mention for the improper browser fingerprinting will be detailed in an extensive discussion in the following subsections.

5.1 Fingerprint

In essence, a fingerprint is a visual projection of the friction ridges on the skin. A friction ridge, otherwise defined as the portion of the digits or the palm that is raised, made from ridge units of friction ridge skin. The traditional approach was to immerse the finger in ink and then press it against a piece of paper that is eventually scanned. Nowadays, live finger scanners are tasked with this and make the task fairly simple and secure. The most popular fingerprint scanners can be found in phones and their task is exactly this: high security at little cost to speed. The approach is based on thermal, ultrasonic, capacitive or optical principles (10; 11; 12).

The optical approach is one of the oldest, existing from 1970s, the principle is simple: the finger is swiped or held over a protective glass which lights and captures the reflected rays from the finger.

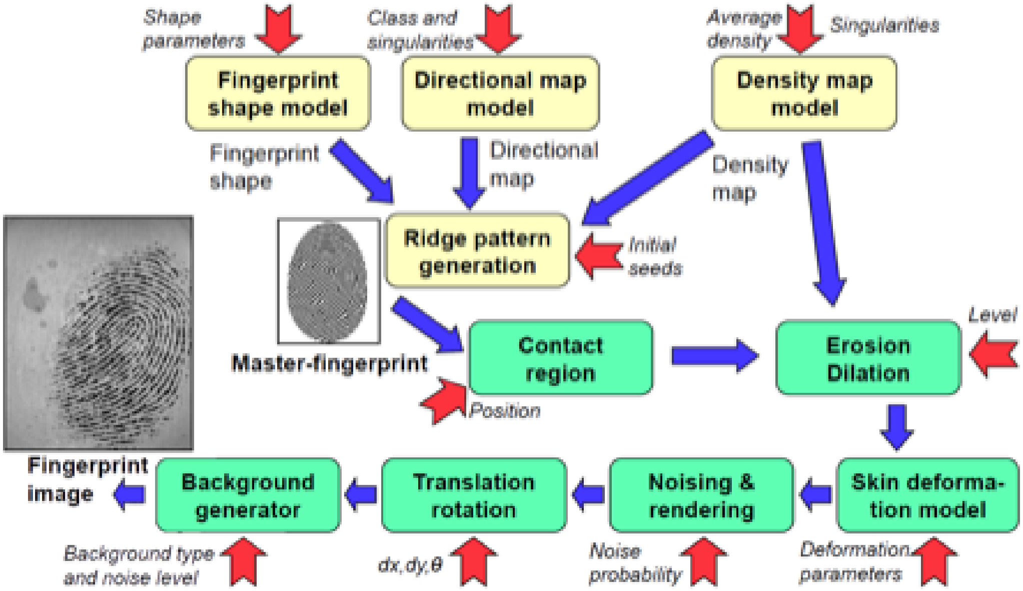
Capacitive approach is to place a two-dimensional array of micro-capacitors plate. There is a danger of damaging the whole device when your finger has electrostatic charge. Also in perspiration there are chemicals that can damage the silicon chip. For these purposes there has to be a protective layer, but this layer has to be as thin as possible to have the smallest impact on the measurement of differences between ridges and valleys.

With the thermal technology, pyroelectric materials generate current according to various temperatures. Ridges have higher thermal radiation than valleys so they have higher temperature. Since temperatures quickly equalise, it is necessary to use sweeping sensors. These are the hardest to implement yet the most secure. Ultrasonic technology capturing devices consist of a transmitter and a receiver. The transmitter sends acoustic signals which are reflected by ridges (skin) and valleys (air) differently. The receiver then receives echo signals and thanks to a different acoustic impedance measures distance and consequently acquires an image of fingerprint. The frequency used by these sensors is between 20 kHz and several GHz. Higher frequencies are helping to get higher resolution. Ultrasonic sensors have one of the best image quality and accuracy rates (10 times better than any other technology). The ultrasonic technology is penetrating the upper part of skin which results in better detection of fake fingers and also it is less influenced by the dirt on fingers (not excepting cuts) or sensors. The main disadvantages are a very high cost and the large size of the device. Another problem is also that the ultrasonic technology cannot operate properly at low temperatures.

Two matching techniques are generally used: Minutiae or Correlation based. Minutiae techniques find the special formation created by papillary lines and maps these points related to the placement on their finger and correlation based techniques usually require the precise location a registration point, being affected by rotation and translation of an image. (6; 7; 8; 9)

5.1.1 Evaluation

The finger print bit map obtained from the reader is affected by the finger moisture as the moisture significantly influences the capacitance .This means that too wet or dry fingers do no produce bitmaps with sufficient quality and so people with unusually wet or dry figures have problems with these silicon figure print readers. The fingerprint bitmap is susceptible to error caused by the finger moisture. Furthermore, Synthetic fingerprint generators are not widely available. (13)



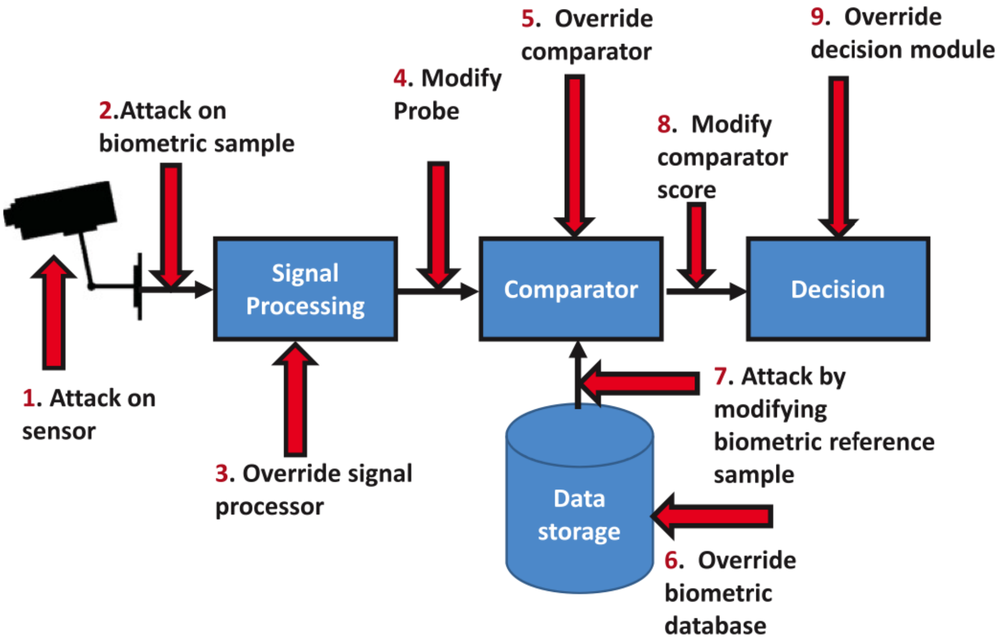
SFinGE: process of fingerprint generation (taken from (14))

5.2 Face Recognition

The way on which the biometric system acquires the image greatly depends on the application underneath. Surveillance applications are best served by capturing videocamera feeds, while some require static images taken by a camera. Other more advanced applications use 3D scanning and infra-red sensors. Therefore we can see three categories of techniques: methods that operate on intensity images, those that deal with video sequences, and those that require other sensory data such as 3D information or infra-red imagery. Due to the recent evolution in video-cameras, facial recognition is now present in some consumer devices.(15)

5.2.1 Evaluation

Generally, multiple vulnerabilities can be found in any system and this is no exception. The figure below shows a block diagram of a generic face recognition system with nine different vulnerabilities, as indicated in ISO/IEC 30107-1:2016 [ISO/IEC JTC1 SC37 Biometrics 2016]. The first vulnerability is noted at the sensor (i.e., the data capture subsystem) and involves presenting a face biometric artifact of the legitimate user as an input to the sensor. An artifact is defined in ISO/IEC JTC1 SC37 Biometrics [2016] as an artificial object or representation presenting a copy of biometric characteristics or syn- thetic biometric patterns. This kind of attack is known as a presentation attack and is defined as a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [ISO/IEC JTC1 SC37 Biometrics 2016]. The second vulnerability is related to intercepting the biometric sample that was captured by the sensor. This attack basically involves replacing the captured face biometric sample with a fake sample. The third vulnerability is overriding the signal processing module. This could involve modifying the functionality of the feature ex- tractor, for instance, using a Trojan horse. The fourth vulnerability allows the attacker to replace the extracted features of the probe sample with target features. The fifth vulnerability involves overriding the comparator so that it will output a comparison score required by the attacker. The sixth vulnerability involves replacing the reference template such that the authorized ID is associated with the attacker template. The seventh vulnerability is the modification of the reference template in the communication channel. The eighth vulnerability is the interception and corruption of the compara- tor output. Lastly, the ninth vulnerability involves overriding the decision module to output the intended decision. Of these nine vulnerabilities, only the first involves an attack on the sensor itself; all the other vulnerabilities are related to the integrity of the overall system.(16)


5. Override comparator
9. Override decision module
4. Modify Probe
2.Attack on biometric sample
8. Modify comparator score
Signal Processing
Comparator
Decision
1. Attack on sensor
7. Attack by modifying biometric reference sample
3. Override signal processor
Data storage
6. Override biometric database

Vulnerability of a face recognition system (inspired by figure in ISO/IEC 30107-1 [ISO/IEC JTC1 SC37 Biometrics 2016]).

5.3 Iris Scan

Iris recognition is the process of automatically recognising and classifying an individual based on the complex iris structure of their iris patterns. Algorithms for iris recognition have proven to be very low FMR and matching with high efficiency in databases of big dimension. This is not a surprise, given the complex textural pattern of the iris stroma that varies significantly across individuals, the perceived permanence of its distinguishing attributes, and its limited genetic penetrance. Multiple studies and reports have highlighted the impressive recognition accuracy of iris recognition in operational scenarios. (17)

5.3.1 Evaluation

Even though some attacks are possible for this biometric method, they are not many due to the nature of the irises and the aliveness detection for irises which is expected. However, it has been noted that imperfect templates generate models that will be venerable. (18)

5.4 Hand Geometry Analysis

A tradeoff between face recognition and fingerprint, idea behind hand geometry scanners is based on the fact that every hand shape is different for everyone and furthermore, this characteristic stops changing in adults. The estimation of width, length, depth as well as skin area are techniques that generally asses hand's movement as well as the way it looks. (19; 20)
This method has grown more secure as well due in part to the advancements in camera technologies as well as 3D imaging systems which handle the data of all features (21; 9; 22)
As with the face recognition systems as well as fingerprint scanners, the processing of the images or 3D mapping is done on a computer, in order to obtain the proper data (23; 24)

5.4.1 Evaluation

This technique requires a lot of conditions to be met and is essentially a method with decreased popularity recently. Requiring the user's hand to be in a specific position in order to work as well as having the issue of the device being unsanitary usually renders this authentication method for lower lever of security requirements. Furthermore, due to the fact that such a small data set is created with the features, only 10-100 bytes of data are occupied depending on the performance of the scanner, rendering this authentication method useless for serious purposes.

5.5 Retina Geometry Technology

This technique is extremely slow and cumbersome, but it generates some of the most accurate results in the field. It requires the user to look into the sensor and focus for a few seconds as the scan completes. A light is projected, illuminating the blood vessels, which are then analysed. As the blood vessels in the retina are a unique pattern, and are not directly visible, this makes for a very accurate technique, with an error rate of more than 1 in 100 000 000 compared to fingerprint's 1 in 15 000. (25; 24) Due to the slow and intrusive nature of the scan, it is not widely used.

5.5.1 Evaluation

With a very small error rates, the remaining drawbacks of this technology are its day to day use the extreme level of intrusiveness, requiring a laser pointed at the cornea, and operation of the scanner either by a human or with an automatic process. Therefore, real world applications of this technique fade away quickly considering the experience of using it.

5.6 Speech Recognition Technique

Speech recognition uses the different features of speech that can be interpreted by a computer such as anatomic or behavioural ones. As speech recognition is not only tasked with assessing the pitch but also the pattern of speech, it is focusing of distinguishing features such as the dimensions of mouth, nasal cavity or tract as well as speed of speaking or the length of pauses. (26; 27) The cost of implementing such a biometric system is low, considering only a microphone is needed to employ it. Also, authentication over distance can be realised by the use of a telephone, an existent technology that can be used as a sensor. (28; 29) And as a result, this field has evolved, employing different methods of recognition such as: Text dependent, where the user basically enrols a spoken password; Text prompted - when there is concern of impersonation (using a recording); Or text independent, where machine learning techniques such as neural networks are employed.

5.6.1 Evaluation

Due to ageing, as voice changes, supplemental changes need to be made for a particular user, but the employing of this method does not require additional hardware and can be used over the phone for remote authentication. However, due to disrupting factors such as background noise or emotional state changes, this method cannot be employed for high levels of security. Nevertheless, automated calls make use of this technique to reduce the workload of phone operators.

5.7 Signature Verification Technique

Counter-intuitively, signature recognition is based on recognising the dynamics of the signature, rather than the final signature form. The means of pressure, direction, acceleration as well as the duration of strokes, their length and number are used to assess muscle memory of the user. This is important, as a signature is public and anyone can forge it. The way this works is simple, either a tablet is used to capture the dynamics of a signature, or the pen itself possesses this capability. (30; 31; 28; 29). There are plenty of disadvantages to this technique, such as users who are not accommodated with this process who will most likely register a signature that is different from their muscle-memory one.

5.7.1 Evaluation

As normal, one will invariably have small variations in their signature, therefore the template for this biometric method should allow for some flexibility. Since most systems record dynamics and not the final signature, accepted signatures may look wildly different from the templates, speed of writing having the biggest weight in assessing this feature, therefore forgery is still a big possibility. In general, with 40 KB of data generated per template (about 10 signatures), this technique has a high failure rate even though it is still used in banks for verification purposes.

5.8 More techniques

5.8.1 Palm-print

With the same amount of rich intrinsic features, such as wrinkles ridges, minutiae, like the fingerprint, palm print sensors have been largely under-used due to the nature of the sensors that have to be quite big in order to achieve their purposes (32; 33; 34). Comparison to other techniques:

- More robust than fingerprints, due to the larger surface
- More difficult to spoof than faces, which are public feature, or fingerprints, which leave traces on many smooth surfaces.
- There is no extra cost required for acquisition (camera)
- It has potential for multi-biometric recognition, as it can be used with other hand-based features

5.8.2 Browser Fingerprinting

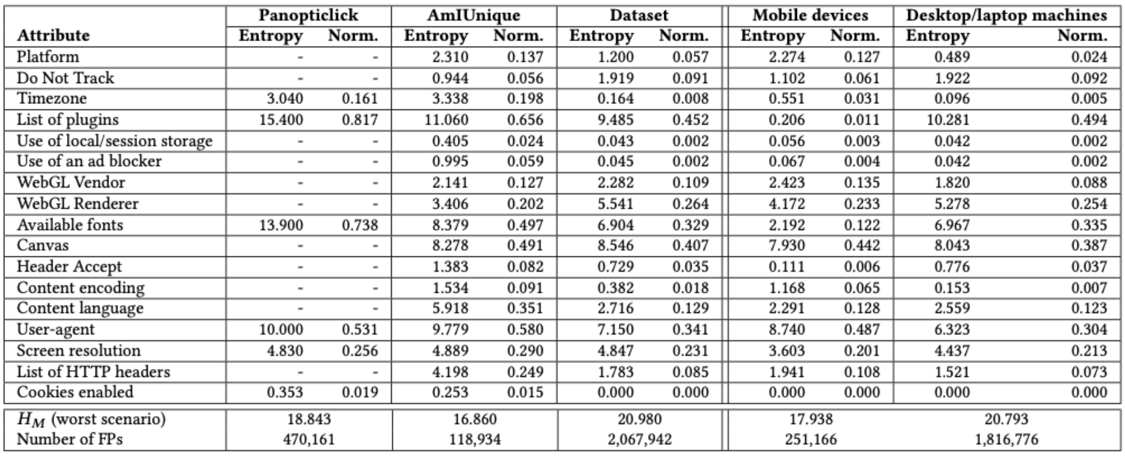
In the early 2010s, it has been proven that data collected by websites is so diverse as well as stable, it can be used to track users across the web. This is done by collecting information from the HTTP headers, JavaScript and install plug-ins. Since then, a race to find new ways to collect even more information as well as to protect against this breach of privacy has begun. In 2016, another study conducted by Laperdrix et al. (**?**) has confirmed the previous findings, though noting a shift in the attributes that are collected. It ha been further demonstrated that the fingerprinting of mobile devices is possible.

Tracking users with fingerprinting is a reality. If a device presents the slightest difference compared to other ones, it can be identified and followed on subsequent visited websites. This can facilitate login, although this is never the end goal if this technique.

The success in identifying a person depends on their platform of choice, for instance smartphones have proven to be more less prone to fingerprinting (18.5%) unique fingerprints found in a data set) than computers (33.6%) (35)

Below, a table of entropy for each data point and for different data sets is shown:

: **Shannon's entropy for all attributes from Panopticlick, AmIUnique and our data.**



	Panopticlick		**AmIUnique**		**Dataset**		**Mobile devices**		**Desktop/laptop machines**	
Attribute	**Entropy**	**Norm.**	**Entropy**	**Norm.**	**Entropy**	**Norm.**	**Entropy**	**Norm.**	**Entropy**	**Norm.**
Platform	-	-	2.310	0.137	1.200	0.057	2.274	0.127	0.489	0.024
Do Not Track	-	-	0.944	0.056	1.919	0.091	1.102	0.061	1.922	0.092
Timezone	3.040	0.161	3.338	0.198	0.164	0.008	0.551	0.031	0.096	0.005
List of plugins	15.400	0.817	11.060	0.656	9.485	0.452	0.206	0.011	10.281	0.494
Use of local/session storage	-	-	0.405	0.024	0.043	0.002	0.056	0.003	0.042	0.002
Use of an ad blocker	-	-	0.995	0.059	0.045	0.002	0.067	0.004	0.042	0.002
WebGL Vendor	-	-	2.141	0.127	2.282	0.109	2.423	0.135	1.820	0.088
WebGL Renderer	-	-	3.406	0.202	5.541	0.264	4.172	0.233	5.278	0.254
Available fonts	13.900	0.738	8.379	0.497	6.904	0.329	2.192	0.122	6.967	0.335
Canvas	-	-	8.278	0.491	8.546	0.407	7.930	0.442	8.043	0.387
Header Accept	-	-	1.383	0.082	0.729	0.035	0.111	0.006	0.776	0.037
Content encoding	-	-	1.534	0.091	0.382	0.018	1.168	0.065	0.153	0.007
Content language	-	-	5.918	0.351	2.716	0.129	2.291	0.128	2.559	0.123
User-agent	10.000	0.531	9.779	0.580	7.150	0.341	8.740	0.487	6.323	0.304
Screen resolution	4.830	0.256	4.889	0.290	4.847	0.231	3.603	0.201	4.437	0.213
List of HTTP headers	-	-	4.198	0.249	1.783	0.085	1.941	0.108	1.521	0.073
Cookies enabled	0.353	0.019	0.253	0.015	0.000	0.000	0.000	0.000	0.000	0.000
H_M (worst scenario)	18.843		16.860		20.980		17.938		20.793	
Number of FPs	470,161		118,934		2,067,942		251,166		1,816,776	

6 Discussion

The reliability of biometric authentication has come a long way in the last 10 years. Due to the advancements of technology and sensors, it is now feasible to completely rely on biometric authentication without a fallback method and rest assured the rate of false accepts or rejects will be much less of a problem than the rate at which passwords are being hacked or forgotten in a classical password paradigm. However, even if in theory every sensor works perfect, it is imperative for a user to have a fall-back password for unexpected cases if the main aim is authentication. For the other use-case of enrolment, the flexibility to use more of these systems is increased, as the security threshold is not that high.

7 Conclusion

Even with the more secure options of face recognition or fingerprint scanning, biometric authentication is far from a perfect solution by any means, like any other security solution. System engineering plays a big part in how the biometric authentication works, since most of the attacks don't focus on the sensor itself but try to find vulnerabilities in the subsequent steps that are taken after the sensor has been used.

However, these are risks that exist with all the other authentication techniques, which don't offer the convenience and usability that biometric authentication does. These problems are especially concerning, when non-repudiation and irrevocability are required for the respective authentication system. Nonetheless, careful application of the biometric techniques leave little to no compromise on security.

Most of the recent privacy concerns with the risk to be identified by anyone if your biometric data is leaked have been mitigated with various methods such as processing of the sensitive data on-device and physically isolating the biometric system from the rest of the computer, essentially treating it like an authority. Furthermore, recent legal developments in the European Union as well as in some other countries, give more power to users in the case that their data is used for purposes that have not previously been agreed to. The General Data Protection Regulation (in the European Union) is a law that takes exactly this matter into hands and aims to deter illegitimate attempts to use one's data.

References

[1] Smart Cart Alliance Identity Council (2007): Identity and Smart Card Technology and Application Glossary, http://www.smartcardalliance.org, as visited on 25/10/2008.

[2] Fosdick, Raymond B. ”Passing of the Bertillon System of Identification.” J. Am. Inst. Crim. L. Criminology 6 (1915): 363.

[3] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, “Biometrics: a grand challenge”, In Proc. of International Conference on Pattern Recognition, Cambridge, U.K., Aug. 2004, pp. 935 - 942.

[4] J. Phillips, A. Martin, C. Wilson, and M. Przybocki, “An introduction to evaluating biometric systems”, IEEE Computer Society., Volume 33, No. 2, Feb. 2000, pp. 56–63.

[5] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., “Biometric Systems: Technology, Design and Performance Evaluation”, New York: Springer Verlag, 2005.

[6] Jain, A. K.; Ross, A. Pankanti, S., ”Biometrics: A Tool for Information Security”, IEEE Transactions on Information Forensics And Security, Volume 1, issue 2, Jun. 2006, pp 125 – 144.

[7] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, “Performance evaluation of fingerprint verification systems”, IEEE Trans. Pattern Anal. Mach. Intell., Volume 28, issue 1, Jan. 2006, pp. 3–18.

[8] A. K. Jain, L. Hong, and R. Bolle, “On-line fingerprint verification”, IEEE Transactions on Pattern Recognition and Machine Intelligence, Volume 19, No. 4, Aug. 1996, pp. 302–314.

[9] L. Hong and A. K. Jain, “Integrating faces and fingerprints for personal identification”, IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

[10] A. Ross, S. Dass, and A. K. Jain, “A deformable model for fingerprint matching”, Journal of Pattern Recognition, Elsevier, Volume 38, No. 1, Jan. 2005, pp. 95–103.

[11] T. Matsumoto, H. Hoshino, K. Yamada, and S. Hasino, “Impact of artificial gummy fingers on fingerprint systems”, In Proc. of SPIE, Volume 4677, Feb. 2002, pp. 275–289.

[12] A. K. Jain, A. Ross, and S. Pankanti, “Biometric: A Tool for Information Security”, IEEE Trans. Information Forensics and Security, Volume 1, No. 2, Jun. 2006, pp. 125–144.

[13] University of Bologna; Biometric System Lab. - WebPage [Online]. 2014 http://biolab.csr.unibo.it/research.asp

[14] Capelli, R. SFinGE; ann Approach to Fingerprint Generation, In BT 2004, International Workshop in Biometric Technologies. Calgary, Canada, 2014, pag-147-154

[15] Jafri, R., Arabnia, H. R. (2009). A Survey of Face Recognition Techniques. Journal of Information Processing Systems, 5(2), 41–68. https://doi.org/10.3745/JIPS.2009.5.2.041

[16] Raghavendra Ramachandra and Christoph Busch. 2017. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. ACM Comput. Surv. 50, 1, Article 8 (April 2017), 37 pages. DOI:https://doi.org/10.1145/3038924

[17] K. Nguyen, C. Fookes, A. Ross and S. Sridharan, "Iris Recognition With Off-the-Shelf CNN Features: A Deep Learning Perspective," in IEEE Access, vol. 6, pp. 18848-18855, 2018, doi: 10.1109/ACCESS.2017.2784352.

[18] Gomez-Barrero, Marta, et al. "Predicting the vulnerability of biometric systems to attacks based on morphed biometric information." IET Biometrics 7.4 (2018): 333-341.

[19] E. Kukula, S. Elliott, "Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance", In Proc. of 35th Annual International Carnahan Conference on Security Technology, UK, Oct. 2001, pp. 83 – 88.

[20] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric", In Proc. of 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, Jun. 2003, pp. 668 - 678.

[21] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through hand geometry measurements,", IEEE Trans. Pattern Anal. Mach. Intell., Volume 22, Issue. 10, Oct. 2000, pp. 1168–1171.

[22] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, "Biometric identification through hand geometry measurements", IEEE Transaction on Pattern Analysis Machine Intelligence, Volume 22, No. 10, Oct. 2000, pp. 1168–1171,.

[23] R. Sanchez-Reillo, C. Sanchez-Avilla, and A. Gonzalez-Macros, "Biometrics Identification Through Hand Geometry Measurements", IEEE Transactions on Pattern Anakysis and Machine Intelligence, Volume 22, Issue 18, Oct. 2000, pp. 1168-1171.

[24] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., "Biometric Systems: Technology, Design and Performance Evaluation", New York: Springer Verlag, 2005.

[25] C. Marin o Æ M. G. Penedo Æ M. Penas Æ M. J. Carreira F. Gonzalez, "Personal authentication using digital retinal images", Journal of Pattern Analysis and Application, Springer, Volume 9, Issue 1, May. 2006, pp. 21– 33.

[26] Kar, B. Kartik, B. Dutta, P.K. "Speech and Face Biometric for Person Authentication", In Proc. of IEEE International Conference on Industrial Technology, India, Dec.2006, pp. 391 - 396.

[27] A. Eriksson and P. Wretling, "How flexible is the human voice? A case study of mimicry," In Proc. of European Conference on Speech Technology, Rhodes, Greece, Sep. 1997, pp. 1043–1046.

[28] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technology, Special Issue Image- and Video-Based Biomet., Volume 14, Issue 1, Jan. 2004, pp. 4–20.

[29] S. Furui, "Recent Advances in Speaker Recognition", In Proc. of First International Conference on Audio and Video based Biometric Person Authentication, UK, Mar. 1997, pp. 859-872.

[30] Samir K. Bandopadhaya, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das, "Statistical Approach for Offline Handwritten Signature Verification", Journal of Computer Science, Science Publication, Volume 4, Issues 3, May. 2008, pp. 181 – 185.

[31] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies”, International Journal of Image and Graphics, World Scientific Publication, Volume 1, No. 1, Jan. 2001, pp. 93-113.

[32] D. Zhang and W. Shu, “Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching”, Pattern Recognition, Vol. 32, No. 4, Apr. 1999, pp. 691-702.

[33] Zhang, D.; Wai-Kin Kong; You, J.; Wong, M, “Online palmprint identification”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 25, Issue 9, Sep. 2003, pp. 1041 – 1050.

[34] Ungureanu, A.S., Salahuddin, S., Corcoran, P. (2020). Toward Unconstrained Palmprint Recognition on Consumer Devices: A Literature Review IEEE Access, 8, 86130–86148.

[35] Alejandro Gómez-Boix, Pierre Laperdrix, Benoit Baudry. Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale. WWW2018 - TheWebConf 2018 : 27th Inter- national World Wide Web Conference, Apr 2018, Lyon, France. pp.1-10, 10.1145/3178876.3186097. hal-01718234v2