# The Aphelion Project

- physical based fingerprint impersonation systems -

**Prerequisites:** In this paper, I will try to define a brief theoretical foundation for biometric based authentication systems with a focus on fingerprinting scanners and follow that up with a basic PoC. In the first part of the project we will not focus on any manufacturers, algorithms or patents, but rather draw the bigger picture. After that, we will pick something more concise to tackle head on. I have no idea right now how this project will turn out, but I am sure it will be great fun.

Usually, I divide my R&D projects in 4 distinct stages:

- RI (general research, light academic papers etc.)
- RII (deep technical research, theoretical foundation, industry knowledge and case studies)
- DI (1st stage of development, mainly derived from books and code snippets found in papers, hacking conferences or contests)
- DII (final PoC, project conclusion)

Now, this project will be a bit different than the usual ones because a hardware component will likely be involved, albeit not necessarily an electronic device – right now I am thinking of designing a collagen or silicone mold resembling a human finger. How will this translate to our workflow? Well, for one, I am pretty sure we will need several iterations until we will be able to register a successful login. Secondly, we need to understand that it's all about probability and margin of errors – no biometric authentication system is perfect.

1. General description

Let us define it in the most basic terms – biometric authentication systems are based on the classic "what you have" principle from systems security design manuals. The basis of such systems is represented by a "token" of uniqueness, a set of characteristics that can be used to differentiate between different actors that might try to gain access to a said resource. Biometric systems use the uniqueness and imperfections of the human body – in our case, skin patterns that are different enough from person to person and thus can represent a reliable way of finding differences **consistently**. The sources for such data can be obtained from fingerprints, voice, facial characteristics, iris or retina, vein patterns. There is a good article on a biometric authentication systems manufacturer that explains the process in an elegant manner: "There are about 30 minutiae (specific points) in a fingerprint scan obtained by a live fingerprint reader. The US Federal Bureau of Investigation (FBI) has evidenced that **no two individuals can have more than 8 common minutiae.**
Recognition decisions in biometric systems must be taken in real-time and, therefore, computing efficiency is key in biometric apps. It is not the case in biometric forensics where real-time recognition is not a requirement." [1]

The biggest threat for fingerprint based authenticators is represented by the ability of altering the biological traits that make those properties unique in the first place – there were cases where plastic surgery or even acids were used in order to alter the results, albeit certain skin disorders can hinder accurate data collection as well.

[2] - Altered Fingerprints of Alvin Karpis

“Fingerprints can be captured as graphical ridge and valley patterns. Because of their uniqueness and permanence, fingerprints emerged as the most widely used biometric identifier in the 2000s. Automated fingerprint verification systems were developed to meet the needs of law enforcement and their use became more widespread in civilian applications. Despite being deployed more widely, reliable automated fingerprint verification remained a challenge and was extensively researched in the context of pattern recognition and image processing. The uniqueness of a fingerprint can be established by the overall pattern of ridges and valleys, or the logical ridge discontinuities known as minutiae. In the 2000s minutiae features were considered the most discriminating and reliable feature of a fingerprint. Therefore, the recognition of minutiae features became the most common basis for automated fingerprint verification. The most widely used minutiae features used for automated fingerprint verification were the ridge ending and the ridge bifurcation” [3]

“Features of fingerprint ridges, called *minutiae*, include:

- ridge ending: The abrupt end of a ridge
- bifurcation: A single ridge dividing in two

- short or independent ridge: A ridge that commences, travels a short distance and then ends
- island or dot: A single small ridge inside a short ridge or ridge ending that is not connected to all other ridges
- lake or ridge enclosure: A single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
- spur: A bifurcation with a short ridge branching off a longer ridge
- bridge or crossover: A short ridge that runs between two parallel ridges
- delta: A Y-shaped ridge meeting
- core: A circle in the ridge pattern" [4]

When it comes to gathering the required data, several roadblocks will need to be bypassed – for one, we will need to make sure that we are using the same setup – same camera, same lightning conditions, same angles and positioning relative to the sensor and so forth. Even minor differences can overthrow the whole project for we will not be able to exploit inconsistent snapshots. Overall, we will not rely on single shot takes – I have not yet decided regarding the equipment nor the methodology, but we only have one day since we started the project, plenty of time for adjustments :).

Given that this is just a hobby project, we will not waste much time considering the performance overhead that our processing will add or the filters that we will be applying to the said pictures, we will keep it simple and start with the most basic image recognition libraries we can get our hands on.

I just took a sneak peek at Gabor filter kernels, found a basic example at scikit [5]. We will get back to it in a couple of days.

Got me about 320 fingerprints (TIFF format) from University of Bologna. 80 of them were synthetically generated [9]. Definitely a good start, albeit the sensors used are a bit old now to be even considered for research. There are 8 different pictures for each person in the dataset, 10 participants in total. At least we now have a basic idea of how our fingerprints should look like before trying to process them.

3rd of October

This morning I spoke with 2 different 3D printing companies here in Bucharest and the consensus was that the fingerprint must be constructed from a 2D image, yet the machines that they had do not offer a very high degree of detail, at least not the level we need in our little project. With that being said, we will try to take a quality 2D snapshot and maybe translate it to a 3D space ourselves. I am not really sure if this is withing our reach technically speaking, but we'll give it a try.

I am currently looking for both synthetic and organic materials, silicon, resins. Things I am looking for:

- **price** (I am an independent researcher; I don't have the budget of making a custom material)

- **ease of use** (toxicity or the need of buying additional equipment will be considered)

- **quantity** (given that we will need more molds, the number of prosthetic molds that we can make using one package will be taken in consideration as well – the higher the better)

- **quality** (we need to be able to take accurate pictures of it in order to build the model)

- **delivery time** (I need them this week, delivery times of more than 2 weeks will severely impact the project's timeline)

I have finally stumbled upon what looks like a reliable provider. I am attaching the list of production partners listed on their website [17]:

**Necumer Gmbh** / **Germany** - Necuron polyurethane and epoxy plates.
**Zhermack SA** / **Italy** - RTV2 platinum silicone, addition silicone, condensation silicone, alginates.
**Altropol Gmbh** / **Germany** - epoxy resins, polyurethane resins, polyester resins, gel pads, release agents, fillers, etc.
**Acrilyc Composite bv** / **Netherlands** - acrylic resins - Acrilyc ONE water based.
**Global Chimica SA** / **Italy** - polyurethane resins elastomers, demolition agents.
**Norelem SAS** / **France** - over 60,000 mechanicals standardized for engineering, maintenance projects.
**OSV Technlogia** / **Ukraine** - dosing / mixing / application tools - composite materials (resin, silicone, truths) and reconstituted stone production lines.

Well, I just ordered some alginate, 10 EUR without delivery. Can't wait for it to arrive. Today I'll read a couple more papers.

I have also saved me some libraries for later use [24].

7th of October

My alginate compound arrived today! Let’s start playing!


I quickly made my first mold:

Nothing exciting on the exterior. Let’s check out the interior.

Looks pretty good to me.

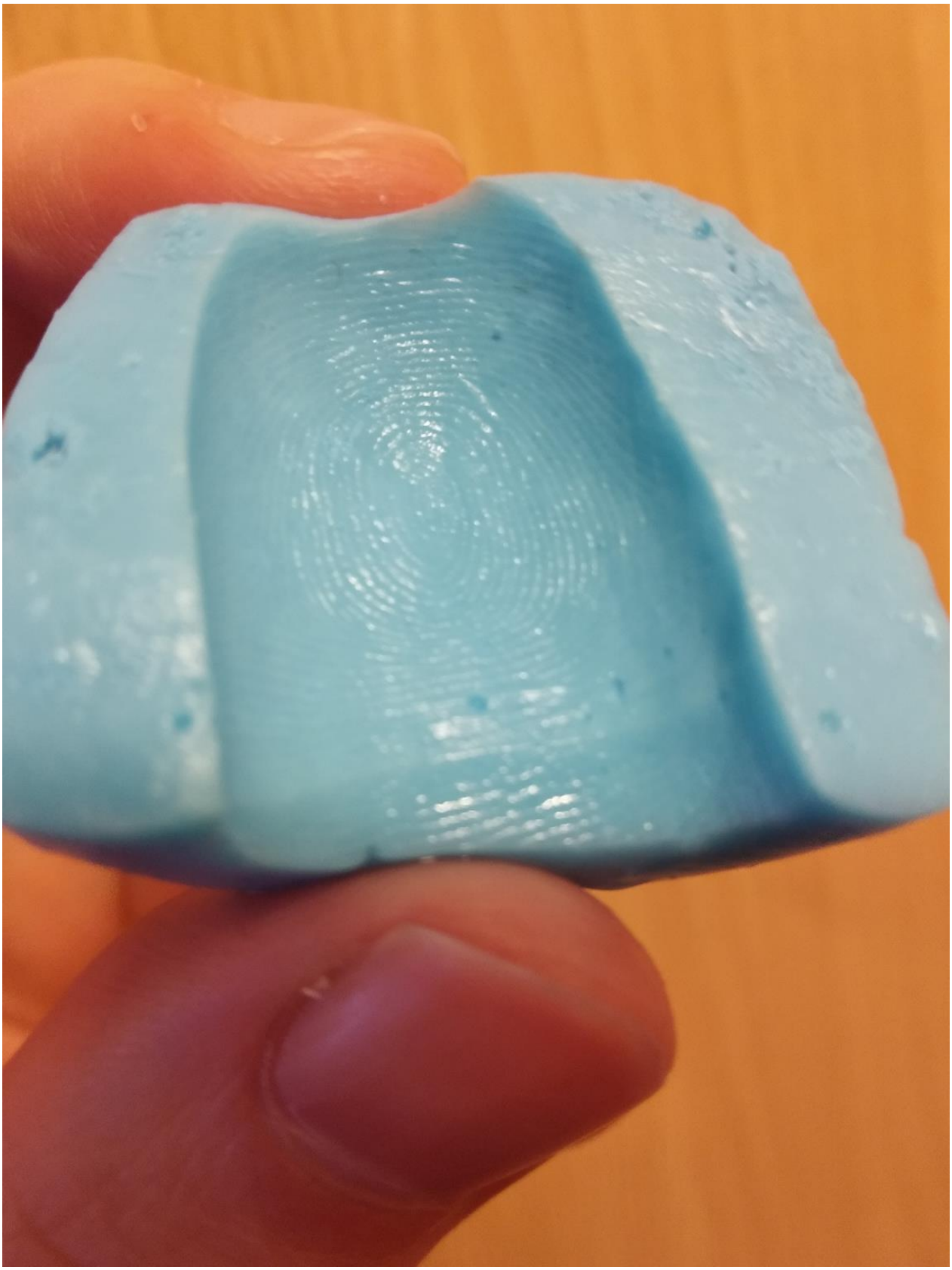
Tried different light conditions:

After making the first login attempt, my mold ruptured and created several micro fissures. On the first 2 or 3 attempts however, my Xiaomi actually **prompted me to reposition my finger on the sensor, thus giving away the fact that it detected that a fingerprint was present** – yet the login was unsuccessful. I tried to replicate the same effect using a different object just to make sure, yet I could only trigger it with the alginate mold.

I decided to make another one:

This time I made a cleaner cut and made the two section a bit thicker.

I am quite satisfied with the results. I also tried different lightning conditions.



We will start the actual image processing tomorrow, for now we should celebrate our small success – the phone recognizes that a fingerprint is shown. We will play with several factors like temperature, humidity in the next days. I want to do one more thing today – apply some basic filters on the fingerprints. I played a bit in Gimp, but the picture quality is bad to say the least. We will continue tomorrow.

Chelălău Ionuț Mihai, R&D Engineer

**Bibliography**:


*1. https://www.gemalto.com/govt/inspired/biometrics*

*2. https://en.wikipedia.org/wiki/Fingerprint#/media/File:Altered_Fingerprints_of_Alvin_Karpis.jpg*

*3. Seong-Whan Lee & Stan Z. Li, eds. (2007). Advances in Biometrics: International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007, Proceedings. Springer Science & Business Media. p. 484*

*4. Davide Maltoni; Dario Maio; Anil K. Jain; Salil Prabhakar (April 21, 2009). Handbook of Fingerprint Recognition. Springer Science & Business Media. p.216.*

*5. https://scikit-image.org/docs/dev/auto_examples/features_detection/plot_gabor.html*

*6. Bergstra J. S., Bardenet R., Bengio Y., and Kégl B. (2011), Algorithms for hyper-parameter optimization, in Advances in Neural Information Processing Systems*

*7. Bergstra J. and Bengio Y. (2012), Random search for hyper-parameter optimization, The Journal of Machine Learning Research*

*8. Snoek J., Larochelle H., and Adams R. P. (2012), Practical Bayesian optimization of machine learning algorithms, in Advances in Neural Information Processing Systems*

*9. http://bias.csr.unibo.it/fvc2002/databases.asp*

*10. Ross Arun A., Jidnya Shah, and Anil K. Jain, Toward reconstructing fingerprints from minutiae points, Defense and Security. International Society for Optics and Photonics, 2005*

*11. OpenCV 3 Blueprints – By Joseph Howse, Steven Puttemans, Quan Hua, Utkarsh Sinha*

*12. Biometric Presentation Attack Detection: Beyond the Visible Spectrum - Ruben Tolosana, Marta Gomez-Barrero, Christoph Busch, Javier Ortega-Garcia Life Fellow, IEEE*

*13. FPD-M-net: Fingerprint Image Denoising and In painting Using M-Net Based Convolutional Neural Networks - Sukesh Adiga V and Jayanthi Sivaswamy*

*14. FDSNet: Finger dorsal image spoof detection network using light field camera - Avantika Singh, Gaurav Jaswal, Aditya NigamIndian Institute of Technology MandiMandi, India*

*15. Fingerprint template protection using minutia-pair spectral representations – Taras Stanko, Bin Chen. Boris Skoric*

*16. Comparison of fingerprint authentication algorithms for small imaging sensors - Mathilde Bourjot, Regis Perrier, Jean Franois Mainguet , CEA Leti – Grenoble Systems Department*

*17. https://www.btools.ro/despre-noi*

*18. Alginate: properties and biomedical applications - Kuen Yong Lee, David J. Mooney*

*19. Review of the Fingerprint Liveness Detection (LivDet) Competition Series: 2009 to 2015 - Luca Ghiani, David A. Yambay, Valerio Mura, Gian Luca Marcialis, Fabio Roli, Stephanie A. Schuckers*

*20. Evaluating software-based fingerprint liveness detection using Convolutional Networks and Local Binary Patterns - Rodrigo Frassetto Nogueira, Roberto de Alencar, Rubens Campos Machado*

*21. Skilled Impostor Attacks Against Fingerprint Verification Systems And Its Remedy - Carsten Gottschlich*

*22. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection - David Menotti, Giovani Chiachia, Allan Pinto, William Robson Schwartz, Helio Pedrini, Alexandre Xavier Falcao, Anderson Rocha*

*23. LivDet in Action - Fingerprint Liveness Detection Competition 2019 - Giulia Orrù, Roberto Casula, Pierluigi Tuveri, Carlotta Bazzoni, Giovanna Dessalvi, Marco Micheletto, Luca Ghiani, Gian Luca Marcialis*

*24. https://www.idiap.ch/software/bob/*

*25. Attacks and Countermeasures in Fingerprint Based Biometric Cryptosystems - Benjamin Tams*

*26.* Bio-Authentication based Secure Transmission System using Steganography - Najme Zehra, Mansi Sharma, Somya Ahuja, Shubha Bansal