Securing Microelectronic Supply Chains with Dendritic Identifiers

Michael N. Kozicki

School of Electrical, Computer and Energy Engineering,
Arizona State University, Tempe, AZ 85287
kozicki@asu.edu

Densec ID LLC, 11811 N Tatum Blvd Suite 3031,
Phoenix, AZ 85028
michael@densecid.com

Provenance – an issue of national security

"…18 newly completed F-35 fighter jets sat outside Air Force Plant 4, … while U.S. Defense Department officials tried to untangle the **supply chain mess** that had stuck them there."

Fake parts: A Pentagon supply chain problem hiding in plain sight, Defense News, December 6, 2022

"An Air Force investigation of a fatal fighter jet crash in 2020 quietly discovered that key components of the pilot's ejection seat **may have been counterfeit**, ..."

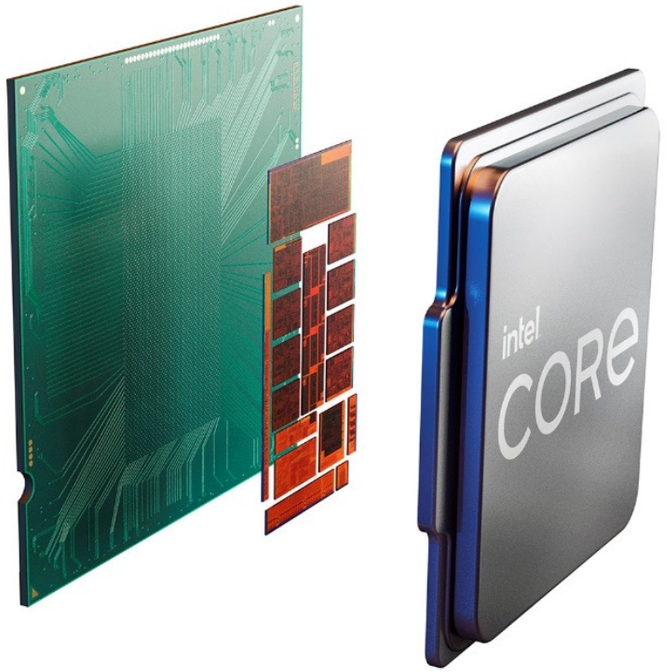
An F-16 pilot died when his ejection seat failed. Was it counterfeit? Air Force Times, September 13, 2022

https://www.defensenews.com/pentagon/2022/12/06/fake-parts-a-pentagon-supply-chain-problem-hiding-in-plain-sight/
https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/

Trust and assurance in microelectronics

"Semiconductor components increasingly require **unclonable and tamper resistant identifiers**, which are especially necessary **as devices become increasingly heterogeneous collections of chiplets and subsystems**.

These **fingerprints provide traceability**, which contributes to process improvements and yield learning and enable tracking for a tightly managed supply chain."



Anne Meixner "Fingerprinting Chips For Traceability"
Semiconductor Engineering, December 12, 2023;
https://semiengineering.com/fingerprinting-chips-for-traceability/

Digital identity – the key to transparency

There are **two components** of **digital identity**:

- The **database** – which holds the information, often in the form of a Distributed Ledger Technology (e.g., *blockchain*) for **data security**.
- The **digital trigger** – this is the physical element that **connects items** in the real world **to their digital presence** in the cloud.

Simple and inexpensive to make and read

Barcodes 

QR codes 

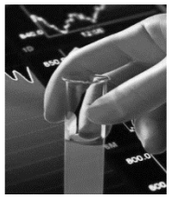
But are easily forged and are not trustworthy

Other issues

- Physical scalability
- Robustness
- Incompatibility with some items
- Require "*personalization*" to give items their own *unique* identity

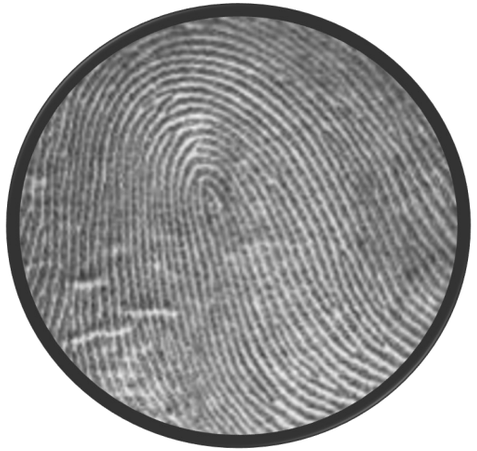
Difficult to copy so are generally secure

 RFID

 Taggants

But are expensive and relatively hard to use

Naturally occurring patterns and identity



Natural patterns are used to identify **people**

Fingerprint

Natural patterns can be used to identify ***things***

Dendritic Identifier

Nature gives these patterns very desirable attributes as **unique identifiers**…

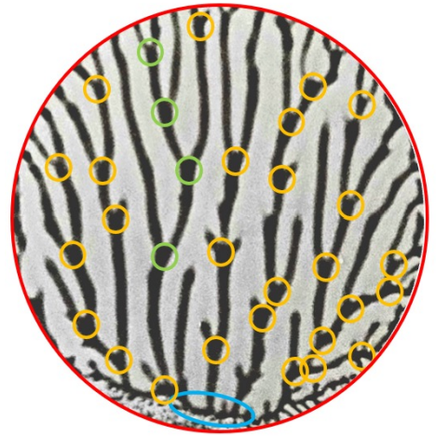
Dendrite: from the Greek *δένδρον*

A structure that develops with a **continuously branching tree-like form**

They are **fractals** with distinct “**keypoints**” which makes them easy to read using computer vision

Dendrites and computer vision

Dendritic keypoints are **nodes** (branching and joining points) and **terminations**.



Keypoints have slightly different **geometry** and **position** for every instance of formation.

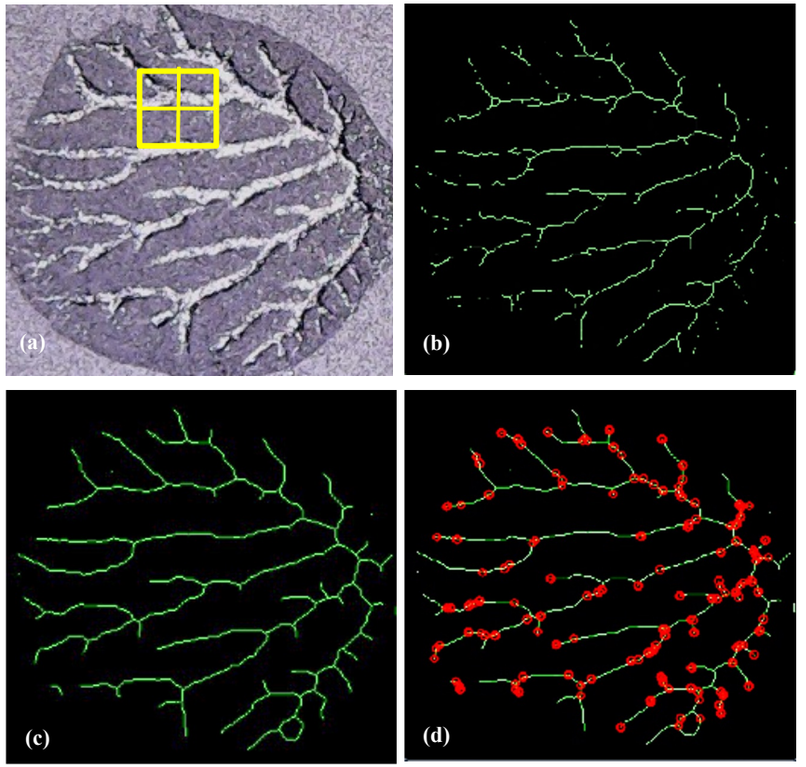
- **Distinctive**: Easily recognizable.
- **Localizable**: Can be accurately located.
- **Repeatable**: Detectable regardless of changes in viewpoint, illumination, etc.
- **Robust**: Invariant to image transformations and noise.
- **Quantity**: Sufficient to describe the pattern uniquely without overwhelming computation.
- **Efficiency**: Detection and classification are computationally efficient for real-time applications.

Informational and structural entropy

Total **number of keypoints** at generation k of the dendrite

$$K_k = \left(S^k\right)^D$$

- For our dendrites $\boldsymbol{S}$ **= 2**
- We can resolve to the 3rd generation, $\boldsymbol{k}$ **= 3**
- Measured fractal dimension $\boldsymbol{D}$ **= 1.7**
- So, we typically obtain **34 strong keypoints**



Taking 2 bits per keypoint (i.e., 4 equiprobable states) gives 4^{34} **>10^{20} possible variations**

But the rule-based pattern has a **low structural entropy**, which allows errors to be detected and repaired (images b and c)

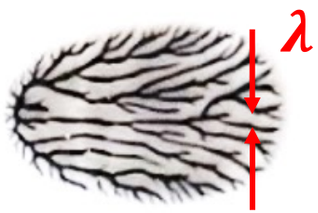
In practice, keypoint detectors (e.g., ORB) can perceive more detail (image d)

Dendrite formation in fluids

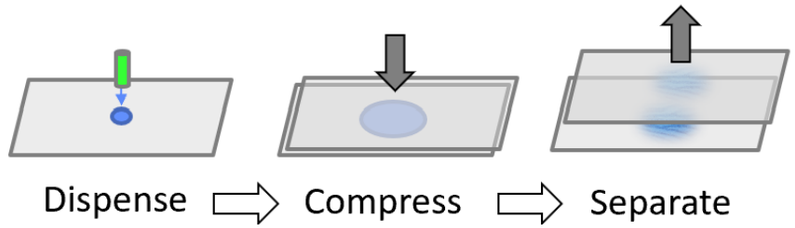
The **Saffman–Taylor** instability is seen when a less viscous fluid is pushed into a more viscous medium.

- The interface moves more quickly at random bulges in the interface where the pressure gradient is highest, leading to a positive feedback effect and “viscous fingering”.
- Leads to a “predictable” rule-based structure with embedded random elements.

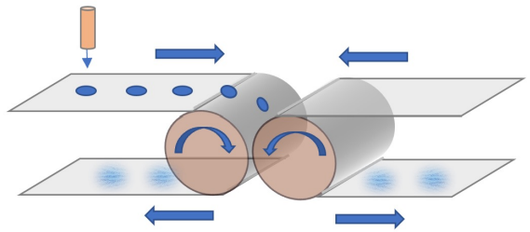
$$\lambda = K_l \frac{b_0 \sigma^{0.5}}{(v^{0.5} \eta^{0.5})^n}$$



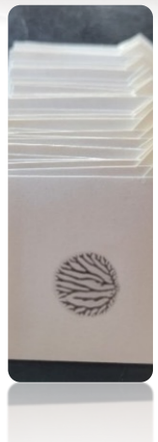
σ = surface tension
η = fluid viscosity
b_0 = compressed fluid thickness
v = separation velocity
K_l and n depend on the geometry of the system and fluid rheology (for stamping, both are dimensionless and close to unity)



***n* = 1** for a lifted Hele-Shaw cell/stamping



***n* = 0.2** for flexo/roll-to-roll printing

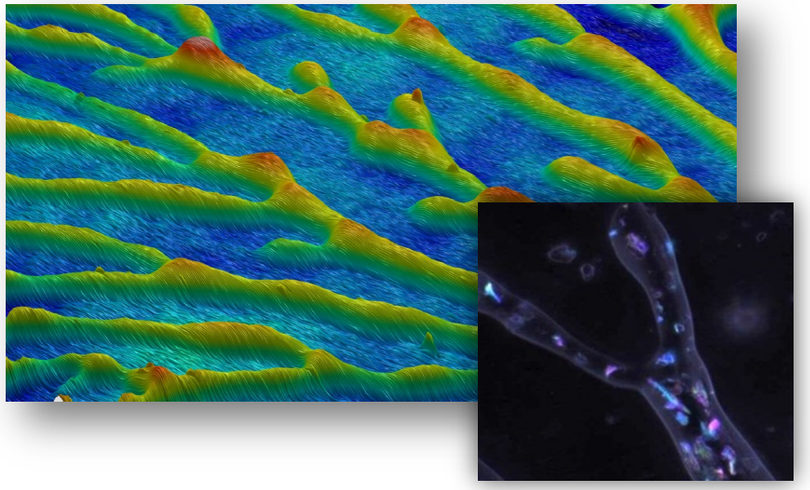


3D security

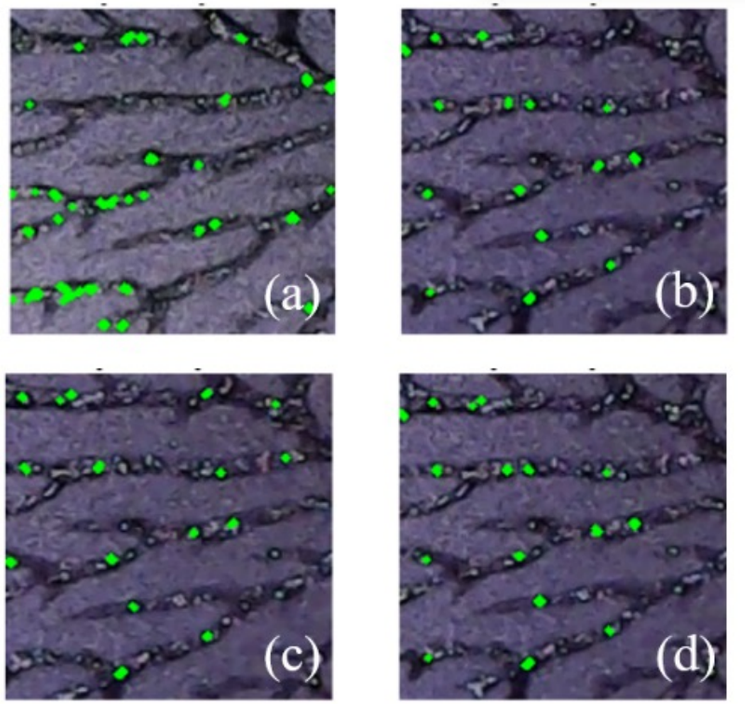
Pattern has a subtle **third dimension** (< 100 µm)

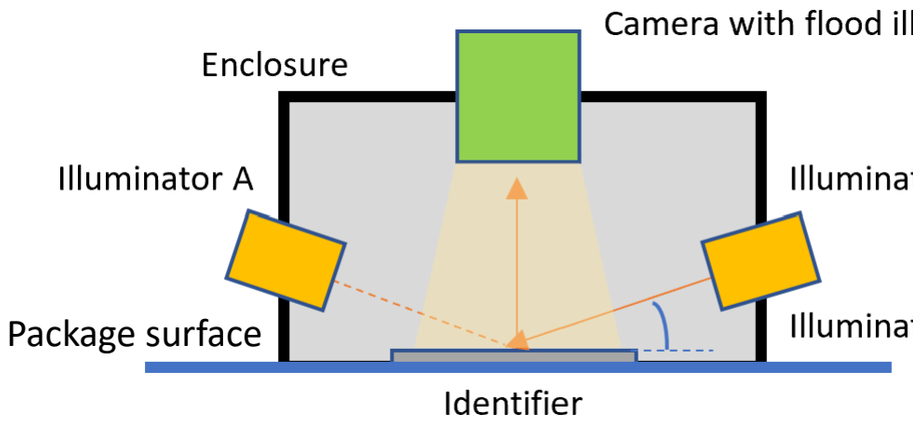
Identifier material is a mixture of a semi-transparent medium and **reflecting flakes**

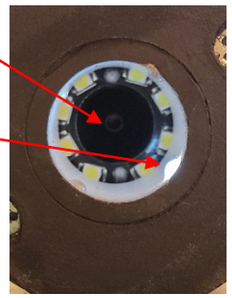
Produces a unique **optical signal** that is **angle dependent** and difficult to fake



- Illumination at 30° L of normal (a)
- Illumination at 30° R of normal (b)(c)(d)
- Get similar “constellations” when illumination is within 10°

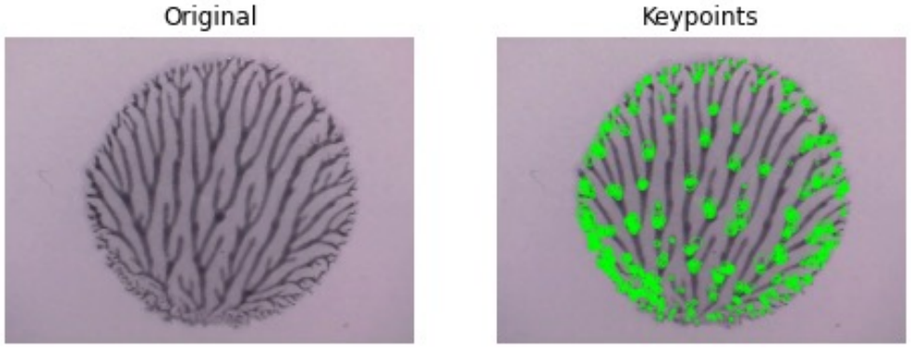




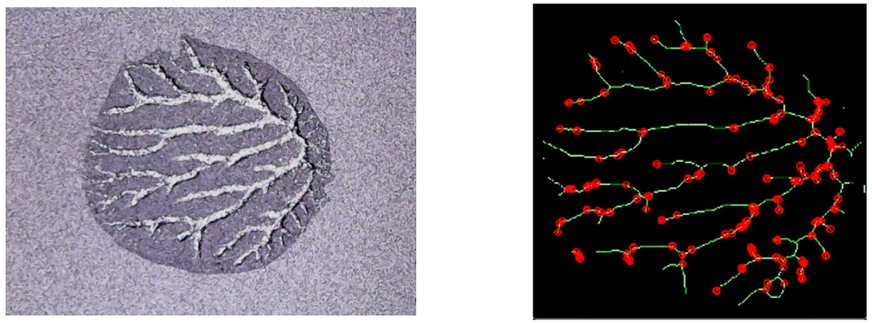


View into enclosure

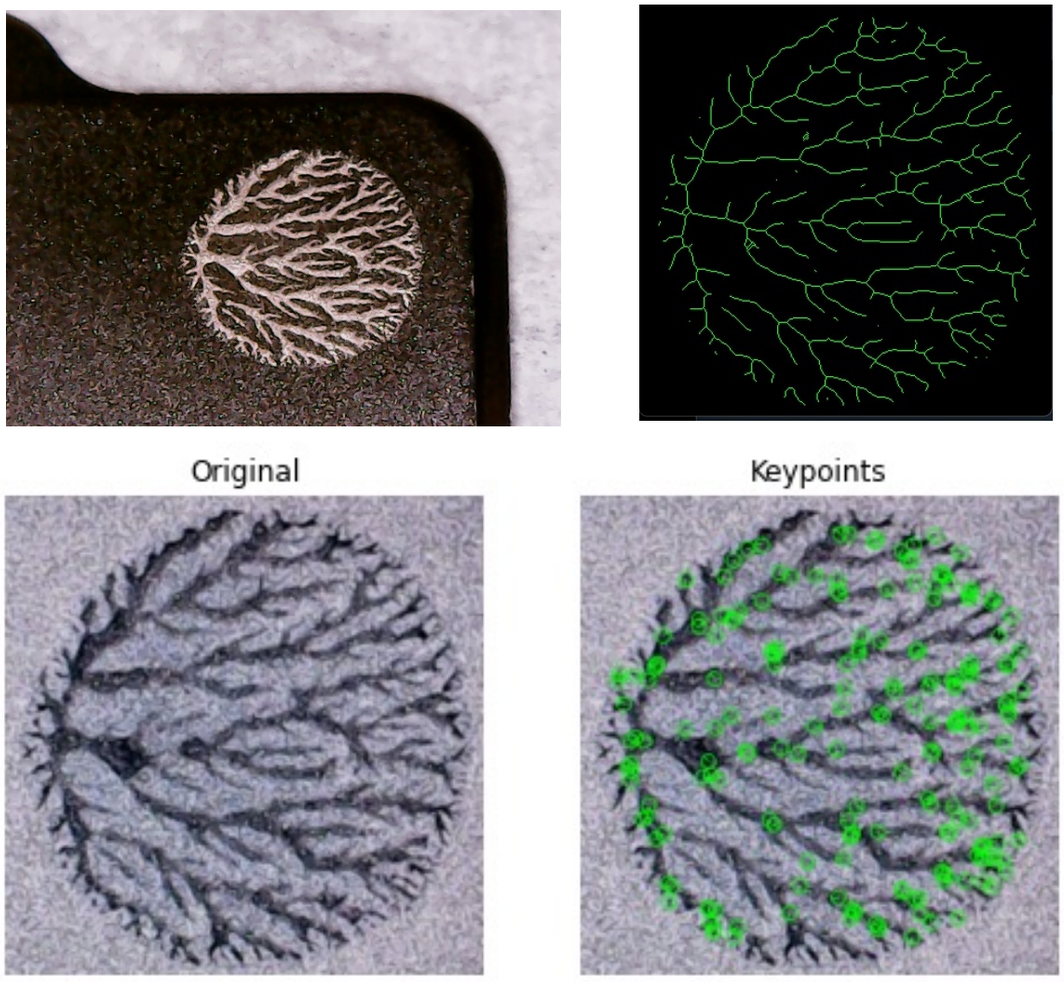
Use examples in IC packaging



Roll-to-roll label-based acrylic DI
for trays and boxes (14 mm)



Stamped removable acrylic + mica DI
on back of silicon chiplet (5 mm)



Stamped high temperature compatible Copprium
Cu-based ink on integrated heat spreader (6 mm)


THANK YOU!