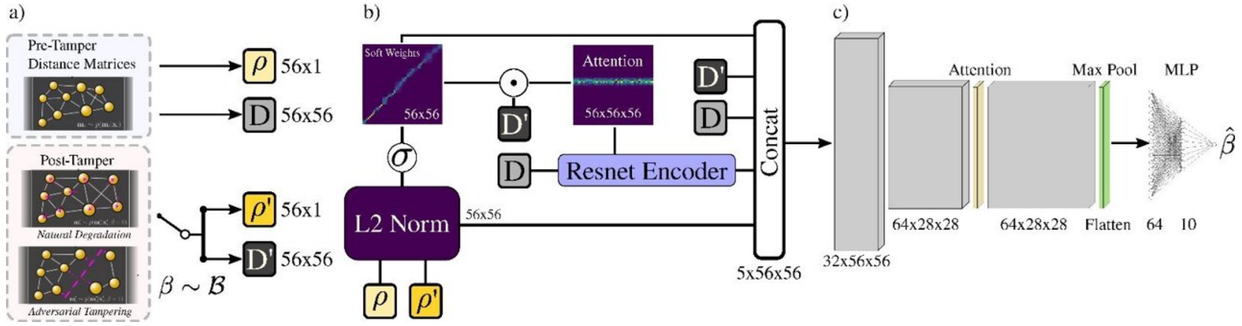
AI-powered optical detection to thwart counterfeit chips

July 20 2024



RAPTOR uses an attention mechanism for prioritizing nanoparticle correlations across pre-tamper and post-tamper samples before passing them into a residual, attention-based deep convolutional classifier. a) RAPTOR takes the top 56 nanoparticles in descending order of radii to construct the distance matrices D and D′ and radii ρ and ρ′ from the pre-tamper and post-tamper samples. b) The radii and distance matrices form the query and value embeddings of an attention mechanism. The attention mechanism is then used alongside the raw distance matrices D′ and D, the softweight matrix, and L2 matrix generated from the radii vectors for the classifier. c) The classifier uses GELU activation and attention layers before applying a kernel layer and max pool layer. Then, the output is flattened into a multi-layer perceptron to compute the final classification. Credit: Blake et al., doi 10.1117/1.AP.6.5.056002

The semiconductor industry has grown into a $500 billion global market over the last 60 years. However, it is grappling with dual challenges: a profound shortage of new chips and a surge of counterfeit chips, introducing substantial risks of malfunction and unwanted surveillance. In particular, the latter inadvertently gives rise to a $75 billion counterfeit chip market that jeopardizes safety and security across multiple sectors dependent on semiconductor technologies, such as aviation, communications, quantum, artificial intelligence, and personal finance.

Several techniques aimed at affirming semiconductor authenticity have been introduced by previous researchers to detect counterfeit chips, largely leveraging physical security tags baked into the chip functionality or packaging. Central to many of these methods are physical unclonable functions (PUFs), which are unique physical systems that are difficult to replicate either because of economic constraints or inherent physical properties.

Rather than being grounded in cryptographic hardness, PUFs emphasize the economic and technological challenges of duplicating a given system's physical characteristics. Optical PUFs, which capitalize on the distinct optical responses of random media, are especially promising. Optical PUFs are easy to fabricate and quick to measure, making them ideal for proof-of-concept tampering identification experiments. Nano-scale metallic optical systems have especially been rising in popularity due to their strong scattering response at optical wavelengths, increasing robustness during post-tampering measurements. However, achieving scalability and maintaining accurate discrimination between adversarial tampering and natural degradation, such as physical aging at higher temperatures, packaging abrasions, and humidity impact, pose significant challenges.

Researchers from Purdue University drew inspiration from the capabilities of deep learning models. As reported in *Advanced Photonics*, they proposed an optical anti-counterfeit detection method for semiconductor devices that is robust under adversarial tampering features such as malicious package abrasions, compromised thermal treatment, and adversarial tearing. They introduced a novel deep-learning approach dubbed "Residual, Attention-based Processing of Tampered Optical Responses" (RAPTOR), a discriminator that identifies tampering by analyzing gold nanoparticle patterns embedded on chips.

The team first built a 10,000-image dataset of randomly distributed gold nanoparticles by augmenting original images from the dark-field microscope. Next, with nanoparticle pattern pixel regions clustered into local particle patterns, their centers of mass are extracted. Finally, the Distance matrix PUFs are generated by evaluating all pairwise distances between these nanoparticle patterns. To test anticounterfeit capabilities, tampering behavior in nanoparticle PUFs was simulated, considering both natural changes and malicious adversarial tampering. RAPTOR, utilizing an attention mechanism, prioritizes nanoparticle correlations across pre-tamper and post-tamper samples before feeding them into a residual, attention-based deep convolutional classifier. RAPTOR demonstrated the highest accuracy, correctly detecting tampering in 97.6 percent of distance matrices under worst-case tampering scenarios, outperforming previous methods (Hausdorff, Procrustes, Average Hausdorff Distance) by 40.6, 37.3, and 6.4 percent, respectively.

This work applied attention mechanisms for deep learning-assisted PUFs authentication. It achieved high verification accuracy under difficult, real-world tampering schema, which opens a large opportunity for the adoption of deep learning-based anti-counterfeit methods in the semiconductor industry.

More information: Blake Wilson et al, Authentication through residual attention-based processing of tampered optical responses, *Advanced Photonics* (2024). DOI: 10.1117/1.AP.6.5.056002

Provided by SPIE

Citation: AI-powered optical detection to thwart counterfeit chips (2024, July 20) retrieved 20 July 2024 from https://phys.org/news/2024-07-ai-powered-optical-thwart-counterfeit.html