Bangjie Sun | Research Statement

My research lies at the intersection of ubiquitous computing, computer vision, and security, with a central focus on trustworthy provenance for physical and digital artifacts. I study how to recover, preserve, and verify evidence about where content comes from, whether it is authentic, and how it has been transformed across its lifecycle.

Trustworthy Provenance for Physical and Digital Artifacts

Modern society increasingly depends on artifacts whose authenticity, origin, and transformation history cannot be verified by human perception alone. Consumers must judge whether physical products are genuine and safe, while creators, platforms, and institutions must determine whether digital content is original, manipulated, or misappropriated. Yet these high-stakes decisions often rely on fragile cues, such as appearance or metadata, that can be misleading, removed, or manipulated. At the same time, the ability to verify such evidence often remains limited to specialized laboratories, proprietary platforms, or expert analysis. As the physical and digital worlds become more intertwined, establishing trustworthy provenance – and making its verification broadly accessible – has become a fundamental challenge for future computing systems.

My long-term research vision is to establish trustworthy provenance across the physical-digital boundary. I seek to build principled, deployable systems that recover, preserve, and verify evidence of an artifact's origin, authenticity, ownership, and transformation history. A central premise of my work is that no single provenance signal is sufficient on its own; instead, trustworthy provenance must integrate complementary evidence from physical signals, forensic traces, and digital records. Equally importantly, I argue that provenance verification should not remain confined to specialized infrastructure. To be truly useful in practice, provenance must also become **ubiquitous**: recoverable, interpretable, and actionable using widely available devices and deployable systems.

My work advances this vision along three connected directions: 1 **provenance of physical products**, where material behavior reveals authenticity and quality; 2 **provenance of digital content**, where intrinsic traces support attribution and origin verification; and 3 **security and robustness of provenance systems**, which ensures these signals remain reliable under adversarial manipulation. Together, these directions aim to make provenance practical and trustworthy for physical products and digital content alike.

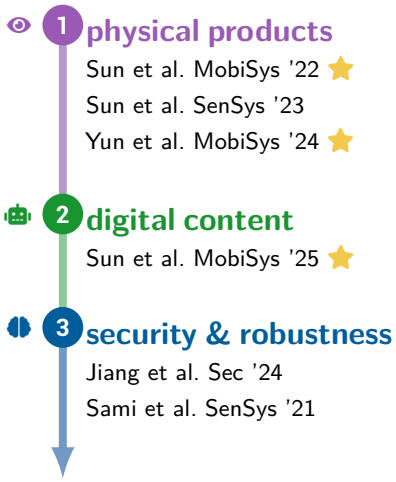
My research has resulted in publications at top-tier venues including ACM MobiSys, ACM SenSys, and USENIX Security (Fig. A), with **one Best Paper Award** and **two Best Poster Awards** accompanying the corresponding papers. A common thread across these efforts is the transformation of everyday devices into provenance tools. Looking ahead, I aim to advance **hybrid provenance** as a unifying framework that combines physical evidence, sensor fingerprints, forensic analysis, and digital or cryptographic records to enable trustworthy reasoning about the authenticity, attribution, and integrity of physical and digital artifacts.

Visible Physics for Trustworthy Provenance

A central theme of my research is that trustworthy provenance must be grounded in evidence that is tightly coupled to an artifact's origin and difficult to fake. At the core of this approach is **Visible Physics** (Fig. B), a methodology that treats commodity cameras not merely as recorders of visual scenes, but as sensors of latent physical and device-level signals. Every image contains traces of how materials behave, how light interacts with matter, and how imaging hardware introduces characteristic imperfections. My research

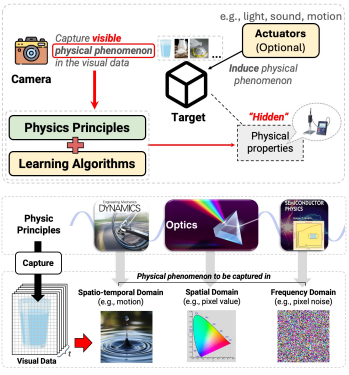
A. Research Overview

My work spans **three tightly connected areas**: **provenance of physical products**, where physical-world signals are used to verify authenticity and quality; **provenance of digital content**, where intrinsic traces support attribution, ownership tracking, and origin verification; and **security and robustness of provenance systems**, which exposes vulnerabilities and strengthens trust under adversarial manipulation.



B. Paradigm of Visible Physics

The figures below illustrate **Visible Physics**, a sensing paradigm that decodes **visual signals** to recover **intrinsic material properties** and other hard-to-observe evidence, transforming everyday devices into intelligent tools for sensing and verification.



leverages these signals as **hard-to-forge evidence** for trustworthy provenance, while emphasizing that provenance verification should be ubiquitous and accessible to everyone rather than confined to specialized instruments or expert analysis. This is why I build on commodity cameras in mobile devices: **by transforming everyday smartphones and cameras into tools for authentication, attribution, and verification, I aim to make provenance evidence universally accessible in everyday life.**

Visible Physics moves beyond black-box AI by grounding sensing and inference in physical principles such as fluid dynamics, optics, and electronics. It exploits observable interactions to recover hidden signals tied to an artifact's material properties, capture process, or source device. Using physics-informed models, I build systems that are more interpretable, data-efficient, and robust than purely appearance-based approaches. This makes Visible Physics a powerful methodology for recovering provenance evidence that is intrinsically linked to origin and difficult to fake.

I have instantiated this paradigm across multiple domains for provenance tasks in both the physical and digital worlds, including *LiquidHash* [3], *FilterOp* [2], and *CAMPrints* [1]. Together, these systems show that Visible Physics can uncover difficult-to-fake provenance evidence from latent signals, enabling more trustworthy verification of the authenticity and origin of physical and digital artifacts.

Recovering Provenance of Physical Products via Smartphones

A major thrust of my research is the **provenance of physical products**: how to recover trustworthy evidence of authenticity and quality from material properties that are invisible to human perception. This problem is both societally important and practically challenging. Consumers often lack reliable ways to distinguish genuine products from counterfeit or substandard ones, even though the consequences range from economic loss to direct risks to health and safety [3, 2, 4]. A key reason is that provenance verification often relies on specialized instruments and expert analysis, making it difficult to deploy at the point of need. My goal is therefore to make such verification **both trustworthy accessible to ordinary users in everyday settings**.

To democratize provenance verification in everyday settings, I instantiate **Visible Physics** through systems that recover difficult-to-fake evidence of authenticity from material behavior using commodity mobile devices. *LiquidHash* [3] analyzes air-bubble behavior in sealed bottles to infer fluid properties relevant to liquid authenticity (Fig. C); *FilterOp* [2] uses a smartphone camera and display to recover optical signals that reveal filtration quality in mask materials (Fig. D); and *PowDew* [4] extends this paradigm to powdered foods by analyzing droplet dissolution behavior. Together, these works show that product provenance can be grounded in latent material properties that are intrinsic to the product and difficult to fake.

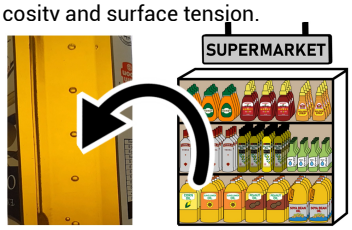
As a result, provenance need not rely solely on labels, packaging, or centralized certification. Instead, by combining physical principles with commodity sensing, we can enable trustworthy and ubiquitous verification of physical products in everyday settings. This line of work has been recognized by a **Best Poster Award at ACM MobiSys 2022** and a **Best Paper Award at ACM MobiSys 2024**, and it establishes a foundation for my broader goal of hybrid provenance across physical and digital artifacts.

Recovering Digital Provenance through Sensor Fingerprinting

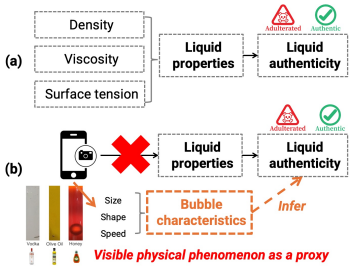
A second thrust of my research is the **provenance of digital content**: recovering trustworthy evidence of origin and ownership when appearance, metadata and other digital cues are no longer reliable. This problem is increasingly urgent, as digital media can be copied, edited, and redistributed at scale, often severing the chain of attribution between

C. Liquid Provenance System

I developed *LiquidHash*, which analyzes the **shape** and **movement** of air **bubbles** in sealed bottles to infer fluid dynamics properties like density, viscosity and surface tension.

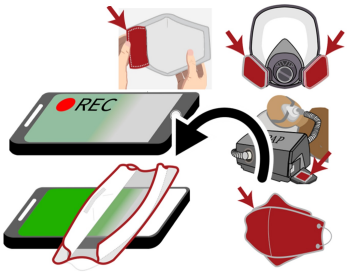


The core idea of *LiquidHash* is to use rising bubbles, a **visible physical phenomenon** induced by human interaction, as a **proxy** to infer liquid content authenticity.



D. Fabric Provenance System

I also developed *FilterOp*, which leverages the smartphone's display and camera to capture **light absorption** and **scattering** effects (i.e., Mie scattering) through filter fibers.



content and its creator [1]. In line with my broader research vision, I seek to make such provenance verification not only robust, but also practical for real-world copyright protection and attribution. To achieve this, I extend **Visible Physics** beyond product authentication to digital media provenance. The key idea is that images do not only depict scenes; they also contain latent traces of the physical device that captured them. In *CAMPrints* [1], I leverage Photo-Response Non-Uniformity (PRNU), a device-specific sensor fingerprint caused by microscopic imperfections in a camera's electrical response, to link digital images back to their physical source (Fig. E). I designed a learning-based system to robustly extract and match these invisible signatures even after common transformations such as cropping, filtering, and recompression.

This work shows that digital provenance can be anchored in physical sensor identity rather than relying solely on fragile metadata or visual similarity. More broadly, it demonstrates how Visible Physics can recover difficult-to-fake evidence not only from material behavior, but also from device-level imperfections embedded in digital content. By linking digital artifacts to the physical process of capture, this line of work advances trustworthy attribution for online media and forms a key bridge in my broader agenda on hybrid provenance across physical and digital artifacts. This work was recognized with a **Best Poster Award at ACM MobiSys 2025**.

Securing Provenance Systems through Vulnerability Discovery

A third thrust of my research studies the **security and robustness of provenance systems**. Trustworthy provenance is only meaningful if the evidence used for authentication, attribution, and verification remains reliable under adversarial pressure. As sensing and inference become increasingly ubiquitous, the boundary between physical signals and digital interpretation introduces new attack surfaces that can undermine both system security and the integrity of provenance evidence. I therefore advocate for **proactive vulnerability discovery** to identify and address such weaknesses before they are exploited.

My collaborative work has exposed critical security gaps in emerging sensing modalities and informed more resilient system design. In *Foice* [5], we showed how facial data could be exploited to bypass voice authentication systems, revealing how signals from one modality can compromise trust in another. In *LAPD* [6], we repurposed smartphone Time-of-Flight sensors to detect hidden cameras, demonstrating how commodity sensing can also defend against physical surveillance. Together, these works reinforce a central principle of my broader agenda: provenance systems must be designed not only to recover useful evidence, but also to remain trustworthy when that evidence is targeted by adaptive adversaries.

Future Research Agenda

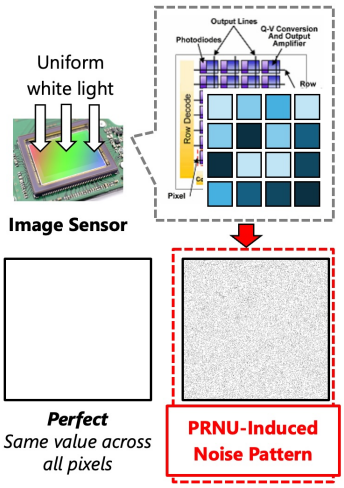
Building on my work on physical product authentication, digital content attribution, and system security, my future research aims to advance **hybrid provenance** as a unifying framework for trustworthy and accessible verification across the physical-digital boundary. **Visible Physics** remains a core methodology for recovering difficult-to-fake evidence, while the broader goal is to **integrate physical, forensic, and digital signals into deployable provenance systems**. I highlight three directions that particularly excite me.

❶ **Ubiquitous Provenance for Physical Products in the Wild.** A key next step in my research is to move product provenance verification from controlled settings into the wild, where real deployment conditions make sensing substantially harder. To do so, I will augment **Visible Physics** with **low-cost multimodal sensor fusion** and **robust inference** (Fig. F). Commodity devices increasingly offer complementary sensing channels beyond RGB imaging, including depth, inertial motion, audio, and Time-of-Flight, which can pro-

E. Sensor Fingerprinting System

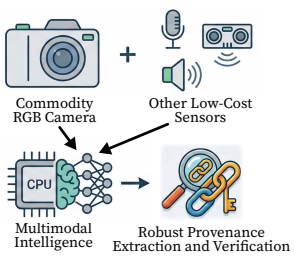
I developed *CAMPrints*, a system that links digital content to its physical identity by leveraging **Photo-Response Non-Uniformity (PRNU)** to combat image theft.

Pixel noises arise from **manufacturing imperfections** and remain inside the resultant images.



F. Multimodal Sensor Fusion and AI

I will augment commodity RGB cameras with **low-cost complementary sensing modalities** and **multimodal intelligence** to enable more robust operation in real-world deployments.



vide additional evidence when visual cues are degraded by motion, lighting variation, occlusion, or limited user cooperation. By fusing these signals with physics-guided, uncertainty-aware inference, I aim to enable reliable, point-of-need provenance verification in everyday settings such as supermarkets, homes, clinics, and field inspections.

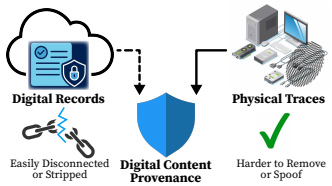
2 Hybrid Provenance for Digital and AI-Generated Content. Building on *CAMPrints* [1], I aim to develop **hybrid provenance** for digital media to foster C2PA-style Content Credentials (Fig. G). C2PA offers cryptographically verifiable provenance, but records can be missing, stripped, or disconnected as media is edited, reposted, recomposed, or generated by AI. I will therefore complement digital records with harder-to-remove physical evidence such as intrinsic capture traces, forensic analysis, and robust fingerprinting, so attribution remains meaningful even when any single signal fails. This is especially important for AI-generated and AI-edited media, where provenance must survive benign transformations and adversarial manipulation across images, video, audio, and multimodal content.

3 Security and Privacy of Provenance Systems. Provenance is only useful if its evidence remains reliable under adversarial pressure and does not create unacceptable privacy risks. I will explore attacks and defenses for provenance systems, including spoofing, laundering, trace erasure, synthetic provenance injection, and cross-modal attacks that exploit interactions between sensing, inference, and media generation pipelines. I will also investigate privacy-preserving mechanisms that enable verification without over-exposing sensitive information. The goal is provenance with clear robustness and privacy guarantees under realistic threat models.

Together, these directions pursue a unified vision: to make provenance **trustworthy, ubiquitous, and deployable** across physical and digital worlds. By combining commodity sensing, physics-guided inference, computational forensics, and secure systems design, I aim to help individuals and institutions reason about the authenticity, origin, ownership, and transformation history of artifacts with confidence.

G. Hybrid Provenance

I will build robust hybrid provenance mechanisms that link edited or generated media to its **origin, creation process, and subsequent transformations**.



References

[1] **Bangjie Sun** Mun Choon Chan, and Jun Han. CAMPrints: Leveraging the "Fingerprints" of digital cameras to combat image theft. In *Proceedings of the 23rd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '25)*, 2025.

[2] **Bangjie Sun** Kanav Sabharwal, Gyuyeon Kim, Mun Choon Chan, and Jun Han. Testing masks and air filters with your smartphones. In *Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23)*, 2023.

[3] **Bangjie Sun** Sean Rui Xiang Tan, Zhiwei Ren, Mun Choon Chan, and Jun Han. Detecting counterfeit liquid food products in a sealed bottle using a smartphone camera. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22)*, 2022.

[4] Jonghyuk Yun, Kyoosik Lee, Kichang Lee, **Bangjie Sun** Jaeho Jeon, Jeonggil Ko, Inseok Hwang, and Jun Han. PowDew: Detecting counterfeit powdered food products using a commodity smartphone. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '24)*, 2024.

[5] Nan Jiang, **Bangjie Sun** Terence Sim, and Jun Han. Can I hear your face? pervasive attack on voice authentication systems with a single face image. In *33rd USENIX Security Symposium (USENIX Security '24)*, 2024.

[6] Sriram Sami, Sean Rui Xiang Tan, **Bangjie Sun** and Jun Han. LAPD: Hidden spy camera detection using smartphone time-of-flight sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21)*, 2021.