Fighting Chip Piracy: IIT Indore's Breakthrough Adds DNA-Based Security to Hardware Designs

A team at the Indian Institute of Technology Indore, led by **Professor Anirban Sengupta** along with **Translational Research Fellow** Aditya Anshul, has developed a cutting-edge technology to strengthen the cybersecurity of hardware IP (Intellectual Property) designs. This innovation is particularly useful for hardware used in multimedia, medical devices, machine learning, and digital signal processing applications. The research has been published in the prestigious journal *Nature Scientific Reports* under the title "Bio-mimicking DNA Fingerprint Profiling for HLS Watermarking to Counter Hardware IP Piracy."

Hardware IP piracy and false ownership claims have become major concerns due to the involvement of multiple players in the global design chain, including IP vendors, system-on-chip integrators, and manufacturing units. There is a growing risk that someone within this chain might illegally copy or falsely claim ownership of IP designs. Often, these stolen designs may even contain harmful logic that escapes quality checks, posing risks to the original creators and end users.

To address these critical issues, the team at IIT Indore has created a technology that uses a DNA fingerprint watermarking method to protect hardware IPs. This technique is based on computer-aided design (CAD) processes and mimics how DNA sequences are uniquely identified in biology. The system automatically generates a unique DNA fingerprint based on the IP vendor's identity, embeds this fingerprint into the hardware design, and acts as a strong digital watermark. This watermark serves as digital proof of ownership and provides strong protection against piracy and fake ownership claims.

The watermarking method works by fragmenting DNA-like sequences, replicating them, and fusing them to create a highly unique DNA signature. This signature is then secretly embedded into the hardware design. The technology is effective in securing various complex hardware designs such as image processing systems, JPEG-CODECs, CNN-based machine learning accelerators, QRS detectors for ECGs, cardiac pacemakers, and digital signal processing units like FIR filters, DCT, and FFT processors.

By embedding this unique DNA-based watermark, the technology ensures that the hardware is genuine and originates from the rightful IP vendor. It is especially useful for preventing malicious actions within the global semiconductor design and manufacturing process. This development is expected to improve trust and transparency in the VLSI semiconductor design chain by helping different stakeholders identify and verify genuine IP designs.

In summary, this innovative solution from IIT Indore aims to protect important hardware designs used in various fields such as multimedia, medical technology, machine learning, and signal processing. The core idea lies in embedding a vendor-specific DNA fingerprint into the chip design, offering a powerful defense against theft and false claims.

Commenting on the innovation, **Prof. Suhas Joshi, Director, IIT Indore**, said, *"This groundbreaking innovation from IIT Indore reflects our commitment to addressing real-world challenges through deep-tech research. Protecting intellectual property in the semiconductor industry is vital for national security and global trust, and this work represents a significant step in that direction."*

Prof. Anirban Sengupta, the Principal Investigator, added, *"Our DNA-based watermarking technology brings a novel layer of cybersecurity to hardware IPs by ensuring that each design carries a unique and verifiable identity. This advancement empowers IP vendors and designers to safeguard their innovations against piracy and misuse across the global semiconductor ecosystem."*