0.1 Abstract

A system for falsifiable process evidence creates tamper-evident records of content creation without relying on content detection or trusted certification. At session start, the system records a capture environment declaration and binds it to every checkpoint. Successive checkpoints are time-locked with verifiable delay functions so they can't be back-dated without real elapsed time. Behavioral binding uses cryptographic keystroke timing (jitter seals) to tie real-time activity to evolving document hashes without capturing keystroke content. Hardware binding can add PUF responses and/or TPM attestation quotes to prove device identity and prevent rollback. Each checkpoint is appended to a Merkle Mountain Range log, signed with a scoped session key, and ratcheted forward so past checkpoints remain safe after later compromise. Evidence is exportable as a portable packet containing inclusion proofs, timing proofs, and optional external anchors. The system enforces adversarial collapse by forcing challengers to allege a specific mechanism and window of fraud rather than vague claims of fabrication.