Abstract

A system and method detect synthetic or simulated keystroke activity by correlating independent data streams in real time. A keystroke-behaviour module evaluates timing, cadence and entropy of keyboard events to flag implausible patterns. An application-context module verifies that each keystroke is appropriate for the foreground window or focused UI element. Parallel screen-content analysis uses OCR and vision on periodic screenshots to confirm that on-screen text, cursor movement or interface changes match the recorded input. A facial-recognition presence module ensures the authenticated user is physically present during typing. An anomaly aggregator combines the module outputs, generates alerts when predefined thresholds are exceeded, and logs all evidence in tamper-resistant records. The multi-channel cross-reference greatly reduces false positives and exposes automated scripts, remote-control sessions and other non-human input sources.