Tamper-Evident Longitudinal Measurement Using a Physically-Unclonable Signature That Is Simultaneously Specimen Identity and Measured Outcome

Applicant / inventor: Cathal Ryan Hynes. The definitions required to practise the present invention are set out in full below; nothing herein incorporates any other application by reference for enablement.

1 Technical Field

The invention relates to tamper-evident longitudinal measurement of a physical specimen, and in particular to a method and apparatus in which a physically-unclonable microstructure signature of a specimen serves at once as the specimen's committed identity and as the measured outcome of a study of that specimen, such that substitution of the specimen is detectable from the evidence record itself without a custody assumption external to that record.

2 Background Art

It is known to authenticate a physical article by a physically-unclonable function (PUF): a random, fabrication-determined microstructure is interrogated and yields a response that is treated as a stable identity, read-noise being removed by a fuzzy extractor or secure sketch operating on committed helper data. In such use the drift of the response over time is ordinarily regarded as a defect to be error-corrected or re-enrolled away, because authentication requires the response to be *stable*. Although certain work exploits ageing-induced change in a physically-unclonable response to detect that a device has been used or recycled, such use makes a one-time determination and does not maintain a committed longitudinal record of the specimen in which the evolving signature is itself the outcome, nor does it render substitution detectable by non-reachability from a committed history.

It has further been proposed to prove physical statements about a pre-characterised disorder-based witness object remotely and without classical secret keys, including the statement that the object has been irreversibly altered or destroyed, the security of such a proof resting on the unclonability of the witness itself. Such proofs are one-shot and binary: any alteration of the witness is the event proved, the object serving as a witness to an external statement rather than as a persistently committed identity, and no committed longitudinal record is maintained in which the evolving signature is itself the measurand; nor is legitimate evolution discriminated from substitution. The acceptance and measurement of on-manifold evolution,

combined with the rejection of off-manifold substitution from the same committed quantity, is by contrast the central teaching of the present invention.

It is also known to provide an article with an unclonable pattern that is deliberately damaged by first use, by a predetermined environmental exposure, or by degradation over time, so that a later mismatch against the enrolled response indicates the article's physical condition or a tampering event; and it has been shown that exposure of an optically complex random medium can irreversibly modify it so that pre- and post-exposure responses prove the occurrence of the exposure, the sensing and the unclonability residing in the same medium. In all such arrangements the change is read as a mismatch, a one-time condition determination, or a binary proof of a single event: the changed response terminates or falsifies the enrolled identity rather than continuing a committed record, no decomposition into an identity-persistent substructure and an outcome-varying substructure is taught, and legitimate evolution is not discriminated from substitution. Likewise, arrangements in which unclonable elements both generate a key and sample an external quantity such as ambient temperature, the sampled readings being stored and signed with the key, keep the measurand a quantity separate from the unclonable response itself.

It is separately known to conduct longitudinal measurement of a specimen – for example under International Council for Harmonisation (ICH) stability protocols, by digital image correlation (DIC), surface profilometry, interferometry, or speckle metrology – and to bind such measurements to a specimen's declared identity by recording an identifier and the measurement as *separate* committed quantities, their association resting on an external chain-of-custody assumption (a logger, a custodian, or a label under institutional control).

The applicant's own earlier applications disclose a projector-detector apparatus (a "Reality Kernel") in which a reactor bearing an unclonable microstructure witnesses an external scene, the two being distinct coupled sub-systems, and in which a committed convolution-bundle record binds a reactor signature to a scene response; a preferred embodiment thereof expressly keeps the reactor and the scene separate, and a materials-characterisation application thereof records specimen identity and specimen measurement as separate committed quantities under an external-custody assumption. No known art teaches a *genesis-committed, longitudinal* record in which a single unclonable quantity, decomposed into an identity-persistent substructure and an outcome-varying substructure, is maintained across epochs so that legitimate evolution is accepted and measured as the outcome while a substitute is rejected as unreachable from the committed history – so that specimen substitution severs the outcome record itself.

3 Summary of the Disclosure

In the present invention the reactor and the scene are one and the same physical volume: the specimen is its own reactor and its own scene, and thereby witnesses itself. The specimen's physically-unclonable microstructure provides, in one committed and irreversibly-evolving quantity $\sigma = (a, d)$, both (i) an *identity-persistent substructure* a that individuates the specimen, and (ii) an *outcome-varying substructure* d whose irreversible evolution is the measured outcome of a longitudinal study of the specimen. Because identity and outcome are read from the same microstructure, substitution of the specimen severs the committed signature chain that constitutes the outcome record itself, so that no custody assumption external to the evidence record is required to detect substitution; in-situ alteration of the genuine specimen is a distinct threat, addressed by a separate sealed-access layer described below.

Before the specimen is assigned to any condition, a genesis commitment $c_0 = H(\sigma_0,\, g,\, K,\, \rho,\, E)$ is formed and published, where σ_0 is the enrolment signature, g a declared coarse geometry, K a committed degradation kernel describing the expected on-manifold evolution, ρ a declared rate bound, and E a committed tolerance envelope. At each subsequent epoch the specimen is re-interrogated to yield σ_t, and the epoch is accepted only if (i) the identity persists, $a_t \in E(a_0)$; and (ii) the change is *on-manifold*, that is, the residual $r_t = \sigma_t - K(\sigma_{t-1})$ is low-rank, correlated with the specimen's own committed prior fine structure, and rate-bounded, $\|r_t\| \le \rho\,\Delta t$, rather than an off-manifold jump. The outcome reading is $y_t = \phi(d_t)$ taken along K. The declared interrogation protocol – including the committed decomposition that separates σ into a and d, the committed registration transform, and the declared outcome map ϕ – is itself bound into the genesis commitment as a committed protocol digest, so that neither the identity/outcome split nor the reported outcome variable can be chosen after assignment; where the protocol digest P is made explicit the genesis commitment is written $c_0 = H(\sigma_0, g, K, \rho, E, P)$.

The distinction that makes this operable is that two manifolds are kept separate and are committed independently: an *identity-continuity manifold* (the reactor projection of the specimen), on which legitimate ageing remains and off which substitution falls; and a *null-expectation manifold* (the scene projection), deviation from which is the measurand. Substitution is detected as departure from the identity-continuity manifold; a genuine outcome – including a genuine novel effect not predicted by the null model – is a departure from the null-expectation manifold that nonetheless remains on the identity-continuity manifold, and is credible precisely because the substitution attack is thereby closed. Discrimination is performed by classical, non-learned analysis against the committed baseline; the invention employs no trained or trusted-third-party verifier. The error and ageing models it does employ are committed in advance, publicly declared, and self-falsifying, and the substitution test rests on self-continuity rather than on the ageing model's absolute forecast, so that operability does not depend on the ageing model being exact.

4 Claim Tier Structure (non-limiting)

The subject matter is disclosed in tiers, which are not transitive: a limitation established for one tier does not propagate to another, and the failure of a conjecture or a non-preferred embodiment does not affect the enablement of the remaining tiers.

Tier A — coincidence and discrimination. The self-witnessing configuration ($\sigma = (a, d)$ from one specimen volume), the genesis commitment before assignment, and the identity-continuity versus null-expectation discrimination, fully characterised in the optical and digital-image embodiments.

Tier B — cross-instrument and batch. Instrument-independent re-reading, and batch protocols with a noise-sized mutual-distinguishability enrolment gate.

Tier C — governance-wrapped and networked. Pre-registration, sealed-access enclosure, separation-of-duties signing, and multi-vantage over-determination.

5 Definitions (self-contained)

The following definitions render the invention practicable without reference to any other application.

Physically-unclonable microstructure signature. A response σ obtained by interro-

gating, with a declared protocol, a specimen whose relevant microstructure is a random, fabrication- or history-determined disorder that cannot be manufactured to specification, such that an independently produced article does not present the same response within the declared tolerance. σ is a vector (equivalently a field sampled on a declared grid) admitting a declared decomposition $\sigma = (a, d)$.

Reactor role; scene role. Two roles occupied, in the present invention, by one and the same specimen volume. In its *reactor* role the specimen's unclonable microstructure is interrogated to yield the committed signature and hence the identity a; in its *scene* role that same microstructure is the object of study, whose irreversible evolution yields the outcome d. The terms are retained from the applicant's earlier apparatus, in which the reactor and the scene are distinct coupled sub-systems; in the present invention they coincide.

Identity-persistent substructure a; fuzzy extraction. The component of σ intended to persist across epochs. A stable identifier is extracted from a noisy read by a committed fuzzy extractor or secure sketch: at enrolment, helper data w_0 is committed such that a later noisy read a_t within a declared error radius reconstructs the enrolled identifier; $a_t \in E(a_0)$ denotes successful reconstruction within the committed tolerance envelope.

Outcome-varying substructure d. The component of σ intended to evolve, whose irreversible displacement is the measurand; $y_t = \phi(d_t)$ is the reported outcome under a declared map ϕ.

Committed degradation kernel K, rate bound ρ, envelope E. A declared predictor of the expected step $\sigma_t \approx K(\sigma_{t-1})$ (the null-expectation model), a declared bound on per-epoch change, and a declared acceptance region; all are fixed in c_0 before assignment and are publicly auditable. K need not be exact: it is used to define on-manifold-ness, and its mis-specification produces systematic, detectable residuals on genuine specimens.

Genesis commitment and epoch chain. A one-way commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ and a one-way hash chain $\chi_t = H(\chi_{t-1}, \sigma_t, \mathrm{meta}_t)$ over epochs; the fuzzy-extractor helper data w_0 committed at enrolment, together with the individual atoms of each committed record, are aggregated under a Merkle root bound into c_0 and are selectively openable. The commit-before-assignment epoch chain is depicted in Fig. 2.

Commit-before-assignment / two-seed opening. The genesis commitment is formed before the specimen is assigned to any condition or before any challenge-selecting value is drawn, so that no committed quantity can be tailored to an outcome or to a later-selected interrogation.

Identity-continuity manifold; null-expectation manifold. Respectively, the set of signatures reachable from σ_0 by continuous evolution of the *same* physical microstructure (correlated with its own committed prior fine structure); and the trajectory predicted by K.

On-manifold residual; substitution. $r_t = \sigma_t - K(\sigma_{t-1})$ is *on-manifold* if it is low-rank, correlated with the committed prior fine structure of the specimen, and satisfies $\|r_t\| \leq \rho\,\Delta t$. Substitution is the presentation of a different physical specimen, whose signature is not reachable on the identity-continuity manifold from the committed history and whose residual is an uncorrelated off-manifold jump.

6 Brief Description of the Drawings

The accompanying drawings are schematic and non-limiting.

Fig. 1 depicts the self-witnessing configuration, in which a single specimen (10) occupies both the reactor role and the scene role of a reactor–scene pair: an emitter (20) and a detector (30) perform a declared interrogation read yielding the committed signature (40) $\sigma = (a, d)$, whose identity-persistent projection a (41) individuates the specimen and whose outcome-varying projection d (42) is the measurand, the genesis commitment (50) being formed before condition assignment.

Fig. 2 depicts the commit-before-assignment epoch chain: the genesis commitment (50) is sealed before the specimen is assigned to any condition (60), whereupon each epoch commits the re-read signature σ_t into a one-way hash chain (70), the identity being checked and the outcome read at each epoch, so that no quantity committed after genesis can be tailored back into c_0.

Fig. 3 depicts the two manifolds kept distinct in signature-space: substitution (96) is a departure from the identity-continuity manifold (90) — an uncorrelated jump — and is rejected, whereas a genuine outcome including a novel effect (94) is a departure from the null-expectation manifold (92) that nonetheless remains on the identity-continuity manifold, and is reported.

Fig. 4 depicts the ageing-versus-substitution discrimination: given the previous committed signature, a residual within the committed acceptance tube (80) that is small, low-rank and correlated with the specimen's own prior fine structure is accepted as legitimate ageing (H_{age}), whereas a large, uncorrelated off-manifold jump is rejected as substitution (H_{sub}).

7 The Self-Witnessing Configuration (the primitive)

The specimen occupies both roles of a reactor-scene pair. In its *reactor* role its unclonable microstructure yields the committed signature and hence the identity a; in its *scene* role the same microstructure is the object of interest, whose irreversible evolution yields the outcome d. Interrogation is by a declared emitter-detector read of the specimen – for example coherent-illumination speckle, digital image correlation, surface profilometry, optical coherence tomography, or spectral read – producing σ_t. Because there is no separate scene coupled to the reactor through a transfer function, no such coupling need be inferred or modelled at verification: the specimen's own evolution is read directly. The coincidence is exact: a and d are projections of one committed quantity σ, so any alteration of the outcome record is an alteration of the identity record and *vice versa*. In some embodiments the same emitter-detector read yields both projections in a single acquisition (Fig. 1). In apparatus terms, the configuration comprises an emitter (20) arranged to interrogate the specimen, a detector (30) arranged to acquire the signature σ_t, and a commitment-and-analysis module configured to form the genesis commitment, to separate the committed signature into the identity-persistent substructure a and the outcome-varying substructure d under the committed decomposition and committed registration transform, to re-authenticate the specimen on a within the committed tolerance envelope at each epoch, and to output d along the committed degradation kernel K as the committed outcome reading, one such emitter–detector read yielding both substructures in a single acquisition.

Substitution is self-defeating by construction: replacing the specimen replaces reactor and scene together, so the freshly-read signature is not reachable on the identity-continuity manifold from c_0, and the committed chain that constitutes the outcome record is severed rather than merely flagged. The invention therefore requires no evidence-external custodian to detect substitution: the article vouches for its own continuity, the distinct threat of in-situ alteration being addressed by the sealed-access layer described below.

8 The Discrimination Problem: ageing versus substitution (technical heart)

A naïve acceptance region – a fixed ball about the enrolled signature – fails, because a legitimately aged specimen leaves the ball while a well-chosen substitute may lie within it. Unconstrained re-enrolment fails symmetrically, because it launders substitution as drift. The invention resolves this by testing *self-continuity* on the identity-continuity manifold, separately from conformance to the null-expectation manifold.

Estimator. At each epoch, form $r_t = \sigma_t - K(\sigma_{t-1})$ and decide between H_{age} (legitimate ageing) and H_{sub} (substitution) (Fig. 4) by (i) a correlation test: the fine-structure of σ_t must remain correlated with the committed fine-structure of σ_{t-1} above a declared threshold (the same grains, defects, and texture evolving); (ii) a rank/energy test: reshaped to a field and reduced by singular-value decomposition, r_t must be low-rank – its energy concentrated in a declared few dominant modes (rank at most a declared $r_{\max}$), legitimate ageing perturbing the microstructure in a spatially-structured, low-dimensional way whereas a fresh substitute yields a full-rank, energy-spread residual – and must satisfy $\|r_t\| \leq \rho\,\Delta t$; and (iii) a boundary-state confidence: the residual is reduced to a scalar decision statistic (a likelihood ratio, or the projection of r_t onto the committed prior fine structure normalised by its read-noise), and a Fisher-information / Cramér-Rao bound on the latent-state estimate fixes the per-epoch state uncertainty from which a detectability index, and hence declared false-accept and false-reject operating points, are computed and logged. An epoch failing both identity persistence and self-continuity places the record in a declared quarantine state. These are classical, non-learned computations executable by an independent party against the committed record; no trained model is used or trusted.

Two manifolds, kept distinct. Substitution is a departure from the identity-continuity manifold (an uncorrelated jump) (Fig. 3). A genuine outcome – including a genuine effect not predicted by K – is a departure from the null-expectation manifold that *remains on* the identity-continuity manifold (the same specimen, evolving anomalously). Accordingly a novel effect is reported, not rejected: an on-continuity, off-null trajectory is a detected outcome whose credibility follows from the continuity test having excluded substitution. The measurand is the projection onto deviation-from-null; the security is the projection onto continuity. Because the discriminator rests on self-continuity rather than on K forecasting the exact aged state, a coarse or imperfect K suffices for substitution detection; operability does not depend on an exact ageing model, and this is a preferred and recited feature.

Scope of the coincidence versus the sealed protocol. The coincidence closes *substitution* (presentation of a different specimen). It does not, by itself, close *in-situ tampering* (deliberate alteration of the genuine specimen to fabricate an outcome), which remains on the identity-continuity manifold. In embodiments requiring that assurance, in-situ tampering is closed by a distinct layer – a sealed-access enclosure, blinded condition assignment, and pre-registration under commit-before-assignment – so that the specimen is committed, its access is physically foreclosed, and any deviation from the committed null is attributable to the declared condition. The credibility of an anomalous outcome is asserted only for specimens that pass self-continuity and were sealed against access.

9 Enablement Machinery

In some embodiments the committed decomposition selects a as an invariant sub-band or set of anchor features (e.g. deep, slowly-varying microstructure or a registration fiducial set) and

d as a displacement field or fast/labile sub-band, with a committed registration transform aligning successive reads and a committed tolerance envelope. A non-destructive committed optical proxy for d may be calibrated against a destructive endpoint assay reserved for that purpose. Rest and recovery paths of the specimen are included in the committed null so that reversible fluctuation is not mistaken for effect. The identity-persistent substructure is selected by the committed decomposition to be substantially invariant over the study window, so that fuzzy extraction operates on a stable source in the conventional sense and is not required to track a moving target; the irreversible drift is confined by the committed decomposition to the outcome substructure. Fuzzy extraction over the invariant substructure thereby provides stable re-authentication while the labile substructure is read as the outcome, the two being separated by the committed decomposition rather than by a learned model. The committed fuzzy-extractor or secure-sketch construction described in detail for the dose-integrating embodiment below – helper data fixed at genesis and bound into c_0, each noisy re-read reconciled against that helper data, corrections outside $E(a_0)$ rejected – is representative and applies, mutatis mutandis, to every embodiment disclosed herein, so that each embodiment need not separately re-teach it.

10 Cross-Instrument Operation

In some embodiments the specimen is re-read on a different qualified instrument. A committed transfer manifest declares the qualified-instrument set and a decomposition of the observed change into an instrument budget (specimen-independent, estimated from cross-reads of an invariant committed reference across the qualified-instrument set), a registration budget (bounded by the committed registration residual), and a genuine-drift budget (the specimen-specific remainder correlated with the committed prior fine structure); the separability constraint requires these three to occupy declared, non-overlapping tolerance subspaces, so that the outcome is instrument-independent within declared tolerance and a re-read on a distinct rig neither creates nor conceals apparent drift.

11 Batch Protocol

In some embodiments an ensemble of specimens is enrolled, each individuated solely by its committed signature, and the batch is admitted only if the committed signatures are pairwise separated by at least a threshold sized against the sum of measurement noise and expected ageing, so that the per-specimen ageing tubes remain mutually disjoint over the study window. Condition assignment is made only after all commitments, in some embodiments by a public-randomness beacon, so that any within-batch relabelling or external substitution is detectable from the evidence record alone. Over- close specimens are recorded in a committed exclusion set.

12 Verifier Audit Protocol

Verification proceeds in two tiers. From the committed record alone, an independent party checks that the epoch hash chain is intact and that the committed trajectory is on-manifold under the declared K, ρ, E; an off-manifold jump in the record indicates a spliced substitution. With the physical specimen available (for example at point of use), a fresh, non-replayable re-read is taken and checked for identity persistence and for landing where the committed trajectory requires; a substituted specimen cannot satisfy this, because its history was never committed. In some embodiments a beacon-selected subset of epochs is

re-measured (spot-check), or a sequential test is applied. All checks are classical and require no trained model and no trusted third party; the custody-free property is a property of the record, not a separate claim over custody.

In some embodiments the interrogation or scan configuration for an epoch (for example a challenge, an illumination setting, or a coverage parameter) is committed to the protocol digest before the corresponding capture is acquired and is not selected from that capture's content, so that no epoch reading can be staged after the fact from its own outcome.

13 Multi-Vantage Over-Determination (hardening)

In some embodiments the specimen is read simultaneously by a plurality of detectors sampling one physical field, and an epoch is accepted only if there exists a field admissible under declared physical constraints – field propagation, material response, and a global passivity or Kramers–Kronig energy-balance constraint – consistent, to within a declared residual tolerance τ, with all detector records on the committed coarse geometry, computed without reference to any committed input-output coupling network; acceptance is a feasibility test – whether the set of admissible fields whose forward-predicted detector responses lie within τ of the records is non-empty – so that no inversion is performed and no unique field need be recovered. The joint record is thereby un-spliceable and its acceptance is model-free in the strong sense, resting on physical law rather than on any fitted model; this hardening is distinct from, and additional to, the committed-model continuity test.

14 Industrial Embodiments

General interrogation loop (canonical embodiment)

In the canonical embodiment the specimen is interrogated in a committed, closed real-time feedback loop, the specimen being at once its own *reactor* and its own *scene*: a single irreversibly-evolving signature $\sigma = (a, d)$ is registered under a genesis commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ formed before the specimen is assigned to any condition, the identity-persistent substructure a authenticating the specimen while the outcome-varying substructure d evolves along the committed ageing kernel K. The industry-specific embodiments set out below are particular cases of this general interrogation loop, each independently enabled and each obtained by specialising the committed interrogation configuration θ – by way of non-limiting example to a fixed scan pattern, a trivial non-adaptive policy, or a single or periodic epoch schedule – the coincidence of identity and outcome and the ageing-versus-substitution discrimination being common to all.

Scanning apparatus (non-limiting). The interrogation is performed by a projector-detector instrument. A controllable emitter – by way of non-limiting example a structured-light projector, a coherent source producing a speckle field, a scanned spot, or a patterned illuminator – directs a probe onto the specimen under the committed configuration θ_t, and a detector – by way of non-limiting example a camera, a photodetector array, or a digital-image-correlation sensor – records the specimen's response. A controller holds θ_t, comprising the emitter pattern, wavelength, exposure, and the region and order of the sweep, commits it to the protocol digest P before the corresponding capture is triggered so that the scan law is bound before the surface is observed, forms the genesis commitment c_0, and appends each epoch's reading to the committed record. In some embodiments the emitter and detector share an optical axis, as a projector-camera pair, so that the instrument both writes the

probe and reads the response; in some embodiments the instrument is fixed on a bench, and in others it is carried by a drone, a crawling module, or a robotic stage that sweeps a large or distributed specimen under committed coverage. The readout modality is selected per specimen class – by way of non-limiting example laser-speckle imaging of a granular or fracture surface, digital image correlation of a strain field, or microscopy of an edge or wear surface – the identity-persistent substructure a and the outcome-varying substructure d being recovered from the same captured field.

Committed adaptive scan policy (non-limiting). In some embodiments the committed configuration θ_t is not a fixed scan pattern but a committed *control policy* governing the scanning spot within the closed real-time feedback loop, so that the principle the scan follows is committed and not merely the captures it yields. In some embodiments the policy is a trained artificial neural network whose committed weights map the instantaneous detector response to control outputs; in some embodiments the policy is realised in an analogue-domain equivalent of the physical-computation kernel of the present family, the committed quantity being an analogue transfer characteristic rather than a set of digital weights. The loop is continuous: the detector response to the current probe drives, by way of non-limiting example, the laser amplitude governing probe intensity, the galvanometer drive voltages governing spot position, and the radio-frequency drive of an acousto-optic deflector governing spot deflection, so that the scanning spot is steered and modulated in real time by the committed policy. Because the policy is configured to reward residual and novelty, the loop densifies sampling on off-manifold or anomalous regions – by way of non-limiting example concentrating captures on newly-appeared corrosion, an incipient crack, or any region departing from the specimen's committed continuity – allocating resolution where the information is greatest. Because the policy itself is committed at genesis or at each epoch, rather than selected from the captured content, this adaptive densification gains coverage on precisely the regions an adversary would seek to conceal without gaining hindsight: the rule that determined to sample a region more densely was bound before the surface was observed, so that a dense scan of a suspect region cannot be dismissed as post-hoc staging, nor an evasive coverage arranged to skip a modification. In some embodiments the committed policy, the resulting per-epoch coverage map, and the captures are all bound into the committed record, so that the adaptivity is itself auditable.

Worked example (committed-θ closed loop, non-limiting). In one non-limiting example a bench instrument interrogates a single specimen, by way of non-limiting example a cutting edge or a wear coupon whose edge microstructure is at once its identity and its wear trajectory. Before each capture the instrument commits a scan configuration θ_t to the protocol digest P, so that θ_t is fixed before it observes the surface and cannot be chosen from the captured content; in some embodiments θ_t is seeded from a public-randomness beacon round not yet drawn at commit time, so that coverage is provably unstaged. The capture yields $\sigma_t = (a_t, d_t)$: the identity-persistent substructure a_t is tested against the committed tolerance envelope $E(a_0)$ for on-manifold continuity under the ageing kernel K, a substituted specimen presenting an off-manifold jump and being rejected, while the outcome-varying substructure d_t is read as the wear signal. The instrument then adapts the next configuration θ_{t+1} from the committed history, closing the loop, but θ_{t+1} is itself committed before its own capture, so that the loop gains coverage without gaining hindsight; where a region cannot be resolved in real time the loop buffers the frame and the omission is evident in the committed coverage record rather than being silently skipped. Because every committed configuration θ and every signature σ are committed in order, the sequence is a self-witnessing longitudinal record: a substitution severs it, and coverage cannot be arranged after the fact to conceal a modified region.

Dose-integrating consumable tag for cold-chain

In some embodiments, the specimen is a consumable dose-integrating tag affixed to, or moulded into, a vaccine, biologic, or blood-product container, in which a single interrogated volume discharges both functions of the invention: the same disordered microstructure that supplies the committed unclonable signature (*reactor*) is the very body whose irreversible evolution is measured (*scene*). The tag comprises a light-scattering matrix overlaid with, or doped throughout by, a dose-responsive layer – for example a radiochromic, phase-change, or photobleaching medium – such that cumulative thermal, ultraviolet, or humidity-time exposure writes a monotone, irreversible displacement into the microstructure itself.

Reading is by coherent illumination: a laser or narrow-band source produces a speckle field whose statistics are decomposed into the committed quantity $\sigma = (a, d)$. The identity substructure a resides in the stable, high-contrast scattering centres and is stabilised for re-authentication by a committed fuzzy extractor, or secure sketch, whose helper data w_0 is fixed at genesis and bound into c_0; at each epoch the noisy re-read is reconciled against w_0 so that ordinary read noise, alignment error, and reader variation are corrected without disclosing a, while any correction lying outside the committed tolerance envelope $E(a_0)$ is rejected. The outcome substructure d is the integrated-dose drift of the same speckle field along the committed degradation kernel K: accumulated excursion advances σ_t monotonically and on-manifold, correlated with the specimen's own prior fine structure, whereas a swapped vial presents an off-manifold field uncorrelated with the committed history and unreachable from c_0 under K at any admissible rate ρ. Substitution therefore severs the signature chain that constitutes the excursion record itself, so no evidence-external custody assumption is required to detect substitution, in-situ alteration of the genuine tag being a distinct threat addressed, where that assurance is required, by the sealed-access layer described in the specification.

This suits WHO and ICH cold-chain governance: a single point-of-use scan simultaneously authenticates the container and reads its accumulated excursion, superseding a separate tamper label together with a separate temperature logger, neither of which is bound to the article it certifies. In some embodiments, the dose-responsive layer is radiochromic and the drift is calibrated to a mean-kinetic-temperature threshold. In some embodiments, the helper data w_0 and the kernel K are borne on the container as a machine-readable code and hashed into c_0. In some embodiments, acceptance additionally requires the reconciled d_t to lie within a committed release envelope, a reading outside it condemning the dose.

Materials ageing, fatigue and creep (digital image correlation)

In some embodiments the specimen comprises a structural coupon of metal, polymer or composite whose free surface bears a random speckle texture, whether intrinsic to the microstructure or applied as a stochastic pattern, and this same surface region is interrogated by digital image correlation (DIC), laser-speckle interferometry or surface profilometry. In such embodiments the committed speckle texture is *simultaneously* the identity commitment and the measured field: one texture discharges two roles. The unclonable spatial arrangement of the speckle, drawn by the committed decomposition from the substantially-invariant coarse arrangement and fiducial sub-band that persists under load, constitutes the reactor signature a, whose genesis commit $c_0 = H(\sigma_0, g, K, \rho, E)$ is recorded before the coupon is placed in service; the progressive displacement and decorrelation of that same speckle under load constitutes the scene outcome d, namely the accumulating plastic-strain, creep and micro-crack field borne by the metal.

Because $\sigma = (a, d)$ is drawn from a single physical volume, the irreversible mechanical damage – fatigue cycles endured, creep strain accrued, fatigue life consumed – presents as a distinct monotone measurand that only advances. In some embodiments acceptance requires that the recovered identity remain within the committed tolerance neighbourhood, $a_t \in E(a_0)$, and that its evolution stay on-manifold under the committed ageing kernel K: a genuine crack propagates as a continuation of the coupon's own prior fine structure, correlated with the speckle already committed, whereas a substituted coupon presents an off-manifold, uncorrelated texture that severs the record. Thus a service log asserting zero hours becomes physically checkable against the metal itself, a pristine ledger being irreconcilable with a strain field the surface plainly carries.

Suitable applications in some embodiments include aerospace life-limited parts, offshore and rail structural members, pressure vessels and additively-manufactured components. In some embodiments the measurand species is fatigue-crack length, creep strain or residual-life fraction; in some embodiments the same surface is over-determined by reading it from a plurality of viewing angles or illumination directions, each independently re-deriving a and d, such that a substitution must defeat every view at once.

Worked example (non-limiting). In one non-limiting example the declared interrogation protocol is as follows. The coupon carries five committed patches of 1024×1024 pixels, imaged by a monochrome camera of at least five megapixels under stable oblique illumination (white light for DIC; a coherent source of wavelength in the range 500–650 nm where laser speckle is used), at a declared standoff and angle repeatable to within declared mechanical tolerances. Each read is normalised in intensity and band-split by a committed linear transform: the identity-persistent substructure a is the low-spatial-frequency band together with a declared fiducial set (features stable under load), and the outcome-varying substructure d is the high-spatial-frequency speckle band, whose inter-epoch displacement and decorrelation fields are the measurand. Successive reads are registered by an affine pre-alignment followed by local DIC refinement, the committed registration residual not exceeding a declared fraction of a pixel. A secure sketch over a (for example a BCH-code construction) is committed at enrolment with its helper data w_0, the declared error radius being set from the replicate-read variance of three enrolment reads; $E(a_0)$ is the corresponding tolerance envelope. The kernel K, rate bound ρ, and envelope E are calibrated from the enrolment replicates together with a declared pilot ageing series on sacrificial coupons of the same material class. At each epoch the residual $r_t = \sigma_t - K(\sigma_{t-1})$ is accepted as H_{age} only if (i) the normalised correlation of its fine structure with the committed prior fine structure meets or exceeds a declared threshold (for example 0.6); (ii) its energy is concentrated in at most a declared number of dominant singular modes (for example rank five); and (iii) $\|r_t\| \le \rho\,\Delta t$; an epoch failing these is classified H_{sub} and the record enters the declared quarantine state. All numerical values above are declared, non-limiting example choices committed in the protocol digest P, selected per material class and modality within the committed calibration procedure.

Pharmaceutical stability study

In some embodiments the specimen is a solid oral dosage form or a lyophilised cake, and the described apparatus is applied to a pharmaceutical stability study conducted under ICH long-term or accelerated storage conditions. The surface microstructure of the tablet or cake – by way of non-limiting example its speckle, granular relief, or pore morphology – functions simultaneously as *reactor* and *scene*. A single committed, irreversibly-evolving signature $\sigma = (a, d)$ is registered for the unit, the commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ being formed

before the unit is assigned to the study and its storage arm. The declared pull-point schedule of the protocol is adopted as the epoch schedule. At each pull the identity component a_t authenticates the physical unit as the unit committed at time zero, acceptance requiring $a_t \in E(a_0)$ together with on-manifold continuity under the ageing kernel K; a substituted unit presents an off-manifold jump and is rejected. The outcome component d_t evolves along K and is read as a degradation-correlated surface signal. In some embodiments a destructive endpoint assay, for example chromatographic determination of related substances, calibrates the non-destructive committed optical proxy, so that d_t reports on chemical or physical degradation without consuming the unit at each pull. Because the commitment precedes assignment, the arrangement closes by construction the attack in which a specimen is exchanged between pulls and the attack in which stability data are back-filled after the fact, discrimination being classical and model-light. In some embodiments the acceptance envelope $E(a_0)$ is widened to admit expected reversible surface changes such as moisture uptake; in some embodiments the epoch schedule additionally records unscheduled temperature excursions for later on-manifold verification.

Forensic exhibit continuity-of-evidence

In some embodiments the specimen is a forensic exhibit, and the described apparatus is applied to continuity-of-evidence. The exhibit's own microstructure – by way of non-limiting example a fracture surface, a tool-mark, paper fibre topology, or ballistic striae – supplies the committed identity, a single irreversibly-evolving signature $\sigma = (a, d)$ being registered for the exhibit with commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ formed at seizure or first examination. The epoch schedule is defined by the custody transfers of the exhibit. At each transfer continuity is re-scored under the committed envelope: acceptance requires $a_t \in E(a_0)$ together with on-manifold continuity under K, while a substituted exhibit or an undocumented intervening handling presents an off-manifold jump and fails continuity. In this way the exhibit vouches for itself, and the human chain of custody becomes a fallback record rather than the base of trust; substitution severs the committed record and requires no external custodian to be detected. In some embodiments the arrangement is distinguished from one-shot object-fingerprinting, which establishes identity at a single instant but does not establish an unbroken, un-spliced longitudinal chain; here the outcome component d_t evolves along K so that the sequence of custody epochs is itself bound into the record and cannot be reordered or interpolated after the fact. In some embodiments the committed envelope $E(a_0)$ is configured to admit benign handling artefacts, such as fresh packaging abrasion, while continuing to reject material substitution; in some embodiments each custody transfer additionally binds a contemporaneous examiner identifier into the epoch record without that identifier becoming the basis of trust.

Biobank and longitudinal clinical specimens

In some embodiments, the specimen is a longitudinal clinical or biobanked biological specimen, such as the cryopreserved contents of a cryovial, an authenticated cell line, or an embedded tissue block. In some embodiments the committed irreversibly-evolving state $\sigma = (a, d)$ is derived label-free from a microstructure intrinsic to the specimen or to its container-contents interface, rather than from a printed label whose issuance an interested custodial institution controls; the identity accordingly attaches to *the vial contents* and not to *the vial*. In some embodiments the commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ is formed before the specimen is assigned to a subject, cohort, or accession, so that the assignment is bound to the physical article rather than merely asserted over it. In some embodiments acceptance

requires $a_t \in E(a_0)$ together with on-manifold continuity of the recovered signature under the ageing kernel K, whereby permitted storage and handling evolve σ continuously along K, while a substitution presents an off-manifold jump that severs the committed record. In some embodiments the outcome coordinate d_t evolves along K to furnish a never-thawed or continuity attestation, freeze-thaw excursions and other custody events being written irreversibly into the committed substructure and read out by classical, non-learned, model-light discrimination. In some embodiments the specimen thereby resists the mislabelling, substitution, and undisclosed re-consenting that constitute the biobank's core provenance fraud. In some embodiments a dependent arrangement authenticates a cell line against cross-contamination by rejecting an off-manifold discontinuity; in a further dependent arrangement the consent status of a human-derived sample is bound to c_0 through a related but distinct governance layer, flagged as such.

Self-certifying calibration standard

In some embodiments, the specimen is a calibration standard or reference artefact, such as a gauge block, an optical flat, or a certified reference material. In some embodiments the artefact's committed microstructure signature a and its calibration-validity outcome d coincide within the single committed state $\sigma = (a, d)$, so that the identity of the artefact and its calibration state are one datum rather than two separately asserted records. In some embodiments the commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ collapses the paper calibration certificate, today issued and held by a trusted third party, into the artefact itself, the certificate becoming a readout of the committed substructure rather than an external attestation about it. In some embodiments acceptance requires $a_t \in E(a_0)$ together with on-manifold continuity under the ageing kernel K; a standard that has drifted or aged out of tolerance is read directly as an on-manifold evolution of d_t along K, while a swapped or counterfeit standard presents an off-manifold jump that severs the committed record and is self-evident under classical, non-learned, model-light discrimination. In some embodiments the artefact thereby renders a drifted or substituted standard self-declaring without recourse to an external certifying authority. In some embodiments this arrangement pairs with a pharmaceutical reference-material embodiment to establish generality across regulated measurement, the committed record supplying metrological traceability. In some embodiments a dependent arrangement supports instrument qualification by binding installation, operational, and performance qualification events to c_0; in a further dependent arrangement an ISO/IEC 17025 calibration interval is enforced by rejecting an on-manifold excursion of d_t beyond a committed tolerance envelope E.

Large distributed structures; vessel self-certification

In some embodiments the specimen is a large distributed structure – by way of non-limiting example a marine vessel, an aircraft, a bridge, a pressure hull, or a building – whose own fabrication- and service-determined microstructure supplies the committed signature, there being no separate reactor: the structure is its own reactor and its own scene, its steel, welds, and coatings furnishing the unclonable disorder while their evolution furnishes the outcome. The committed signature $\sigma = (a, d)$ is drawn from a plurality of committed patches distributed over the structure and read by a projector-detector instrument, in some embodiments carried by a drone or a crawling module that sweeps the structure. The identity-persistent substructure a is selected as the deep, slowly-varying structural fingerprint – by way of non-limiting example weld-bead topology, plate-boundary layout, hull-form geometry recovered by photogrammetry, and deformation history at committed fiducial patches –

while the outcome-varying substructure d is the surface and near-surface state, by way of non-limiting example corrosion, coating craquelure, and modification.

The genesis commitment $c_0 = H(\sigma_0, g, K, \rho, E)$ is formed at a declared enrolment event, in some embodiments the registration or commissioning of the structure, so that the registered identity of the structure is its self-witnessing signature rather than an applied marking. Because the greater part of the structure is unchanged at any epoch, the unchanged regions anchor the correlation that establishes self-continuity: a repaint, re-plating, or refit presents as a localised, committed, on-manifold event reachable from the committed history under K only at a per-epoch change no greater than $\rho\,\Delta t$ and only where the changed region remains correlated with the persisting committed neighbourhood that anchors it, so that even a piecewise substitution staged across epochs cannot remain on-manifold; and the structure remains the same structure through gradual replacement, its identity residing in the unbroken committed continuity of its evolving signature rather than in the persistence of its matter. By contrast, presentation of a different structure yields a signature uncorrelated with the committed history – an off-manifold jump that severs the record – and a structure reconstructed from removed components, having no committed continuity chain, likewise fails self-continuity. The arrangement thereby resolves, for a physical structure, the classical problem of identity through gradual replacement.

In some embodiments the scanning instrument operates an adaptive coverage loop in which a scan configuration θ_t is committed to the protocol digest before the corresponding capture is acquired, and is not selected from that capture's content, so that coverage cannot be staged after the fact to avoid a modified region: the scan law is bound before it observes the structure it inspects, and any omitted region is evident in the committed coverage record.

This suits the detection of vessel-identity fraud – by way of non-limiting example the re-registration of a repainted or re-numbered hull, the substitution of a hull under a retained identity, and the laundering of a stolen or sanctioned vessel – none of which can reproduce the committed continuity of the genuine structure however faithfully an applied identifier is copied. In some embodiments the structure is a marine vessel and the arrangement furnishes a self-witnessing identity for a flag-state registry, a classification society, or a marine insurer; in a further dependent arrangement the committed coverage record produced under committed scan configurations θ_t is a required output of each epoch; in a further dependent arrangement the enrolment event is bound to a public-randomness beacon so that the enrolment time is itself attested.

Anti-counterfeit lot-release (illustrative; dependent only)

In some embodiments a lot-release registry authenticates goods by the same committed signature that reports their degradation trajectory, a degraded-genuine article being distinguished from a counterfeit by the committed on-manifold history rather than by identity alone. This embodiment is disclosed as illustrative and dependent, the anti-counterfeit application of an unclonable signature being otherwise known; the inventive contribution recited elsewhere resides in the coincidence of identity and outcome and in the ageing-versus-substitution discrimination, not in bare anti-counterfeiting.

15 Governance Interoperation (non-limiting)

In some embodiments the foregoing is operated within a governance framework providing pre-registered hypothesis families with committed null encoders, sealed-access enclosure,

blinded and beacon-assigned conditions, separation-of-duties signing identities for design, budget and review, and a two-tier standing-versus-instance state machine; confirmed null results are published under the same commitment discipline as confirmed effects. These governance elements are recited for combination only and are not essential to the Tier-A subject matter.

16 Further Disclosures and Improvements (independently severable)

The following are disclosed as independently severable improvements and are not essential to the foregoing: a directed-dominance declaration test for asymmetric drive-response coupling (a directed-dominance margin together with a bounded back-transfer condition); an attested- communication deception measure admitted only above a certified translator round-trip error bound; a one-sided spatiotemporal-consistency penalty that vanishes for physically admissible sub-luminal propagation; a query-throttle whose engagement tracks the measured high-sensitivity region of a learning curve; a dynamical-hardness certificate reporting a positive-Lyapunov / irreversibility statistic as a pass/fail qualification of a substrate's exploitable unclonability; and a certified few-shot commissioning procedure. Each is disclosed for its own sake and may be practised independently of the self-witnessing subject matter.

17 Industrial Applicability

The disclosed method and apparatus are applicable to at least the following fields: cold-chain and dose-integrity monitoring of vaccines, biologics and blood products; materials ageing, fatigue and creep assessment of aerospace, offshore, rail and additively-manufactured structural components; pharmaceutical stability studies under ICH long-term and accelerated conditions; forensic exhibit continuity-of-evidence; biobank and longitudinal clinical specimen provenance; self-certifying calibration standards and reference materials; self-witnessing identity for large distributed structures including marine vessels, aircraft, bridges and pressure hulls; and lot-release authentication of goods against a committed degradation history. In each field a single interrogated specimen volume serves at once as its own committed identity and as the measured outcome of its own longitudinal study, so that substitution is detectable from the evidence record itself without a chain-of-custody assumption external to that record.

18 Non-Limiting Statement

The embodiments and numerical, material, and modality choices above are illustrative and non-limiting. Governance nomenclature is optional naming over mechanism. No theoretical conjecture is relied upon for enablement; all estimator recipes are engineering choices within declared envelopes. The invention resides in the combinations of technical features disclosed, and extends to all equivalents thereof.