Description
Titre de l'invention : Protocole et système de validation de réalité physique comprenant des procédés utilisant une pluralité de sources et de dispositifs de capture avec recoupement synchronisé des données, et ensemble de techniques de vérification complémentaires

DOMAINE TECHNIQUE

La présente invention concerne le domaine de la vérification d'intégrité physique, de l'authentification de présence, et de la validation de réalité à distance.

Plus particulièrement, l'invention se rapporte aux systèmes et procédés permettant de confirmer qu'une scène, un sujet humain, un objet, ou une situation observée à distance correspond à une réalité physique authentique, et non à une simulation, reproduction, ou manipulation numérique.

L'invention trouve des applications dans, mais sans s'y limiter :

A) Vérification d'identité et de présence humaine :
- La vérification d'identité biométrique
- La détection de présence physique (liveness detection)
- La vérification de présence humaine réelle sans identification (proof-of-human), incluant, sans s'y limiter : inscriptions sur services en ligne, création de comptes, accès à des ressources
- La vérification anonyme ou semi-anonyme (confirmation qu'un sujet est un être humain réel et physiquement présent, avec ou sans divulgation de son identité, avec ou sans association à une identité officielle)
- La preuve d'unicité humaine (un individu physique = un compte ou une entité, sans nécessairement connaître l'identité de cet individu)
- La distinction humain/machine (alternative ou complément aux CAPTCHAs et systèmes de vérification automatisés traditionnels)
- L'anti-usurpation d'identité (anti-spoofing, anti-impersonation)
- La confirmation de présence et/ou d'intention pour opérations à enjeux élevés (incluant, sans s'y limiter : actes juridiques, transactions financières, décisions corporatives, ou tout contexte où l'authenticité de la volonté de l'acteur doit être établie)

B) Vérification d'objets et de documents :
- La vérification d'authenticité d'objets à distance (tels que, sans s'y limiter : oeuvres d'art, objets de collection, produits de luxe)
- La vérification d'intégrité de documents physiques
- L'inspection d'objets de valeur dans des espaces sécurisés (tels que, sans s'y limiter : coffres-forts, réserves de musées, salles bancaires)

C) Vérification de lieux et de scènes :
- L'état des lieux immobiliers à distance (incluant, sans s'y limiter : entrée/sortie de locataires, constats d'inventaire)
- L'inspection à distance de locaux ou d'installations
- Les constats de sinistres ou d'incidents (incluant, sans s'y limiter : assurances, expertises, litiges)
- La vérification de l'intégrité d'espaces sécurisés

- La documentation de scènes pour preuves juridiques

D) Applications générales :
- Toute application nécessitant la confirmation qu'une capture audiovisuelle provient d'une réalité physique et non d'une source synthétique ou manipulée
- Tout contexte où la manipulation numérique d'une scène représente un risque

ÉTAT DE LA TECHNIQUE

2.1 Contexte général

Dans le contexte actuel de numérisation croissante des services et des interactions, la nécessité de vérifier à distance l'authenticité d'une personne, d'un objet, ou d'une situation est devenue critique. Les domaines bancaires, juridiques, médicaux, et administratifs requièrent des moyens fiables pour confirmer que l'entité observée via une capture audiovisuelle est bien réelle et présente physiquement.

Parallèlement, les technologies de génération et manipulation d'images et de vidéos ont connu des avancées majeures. Les techniques dites de "deepfake", les moteurs de rendu en temps réel, et les outils d'intelligence artificielle générative permettent désormais de créer des contenus visuels synthétiques difficilement distinguables de la réalité.

Cette situation crée une "course aux armements" perpétuelle entre les technologies de vérification (détection) et les technologies de falsification (génération), où chaque avancée d'un côté entraîne une réponse de l'autre.

2.2 Solutions existantes

Les solutions actuelles de vérification de présence et d'authenticité reposent principalement sur :

a) Analyse d'image par intelligence artificielle :
Des modèles entraînés tentent de détecter des artefacts visuels caractéristiques des contenus générés ou manipulés. Ces systèmes analysent la texture de la peau, les reflets, les micro-mouvements, et d'autres caractéristiques visuelles.

b) Capteurs de profondeur (mono-dispositif) :
Des dispositifs équipés de projecteurs de points infrarouges ou de caméras stéréoscopiques intégrées tentent de vérifier la tridimensionnalité du sujet. Exemples : Face ID (Apple), capteurs de profondeur Android.

c) Défis actifs (challenges) :
Le système demande à l'utilisateur d'effectuer des actions spécifiques (tourner la tête, cligner des yeux, sourire) et vérifie la cohérence de la réponse.

d) Flash d'écran et analyse de réflexion :
L'écran du dispositif émet des séquences lumineuses et le système

analyse les réflexions sur le visage de l'utilisateur.

Les solutions actuelles présentent les inconvénients suivants :

- VULNÉRABILITÉ À L'AMÉLIORATION DES GÉNÉRATEURS : Les systèmes basés sur la détection d'artefacts sont voués à devenir obsolètes à mesure que les technologies génératives s'améliorent. Un détecteur entraîné sur les artefacts de 2024 sera inefficace contre les générateurs de 2026.

- LIMITATION MONO-DISPOSITIF : Toutes les solutions actuelles opèrent sur un dispositif unique, permettant à un attaquant de compromettre ce seul point de capture (injection de flux vidéo, émulation de capteurs).

- ABSENCE DE VALIDATION PHYSIQUE CROISÉE : Les systèmes actuels ne peuvent pas vérifier la cohérence géométrique, photométrique, radiométrique, et télémetrique d'une scène vue depuis plusieurs angles indépendants simultanément.

- COÛT COMPUTATIONNEL DE LA DÉTECTION VS GÉNÉRATION : Détecter un contenu falsifié requiert une analyse complexe, tandis que générer un contenu falsifié devient de moins en moins coûteux. Ce déséquilibre favorise structurellement les attaquants.

- ATTAQUES PAR INJECTION : Un attaquant peut intercepter le flux de données entre le capteur physique et le logiciel de vérification, injectant un flux synthétique qui contourne entièrement les capteurs réels.

2.3 Problème technique à résoudre

Le problème technique que la présente invention vise à résoudre est le suivant :

Comment concevoir un système de vérification d'authenticité et de présence physique qui :

1. Ne repose pas principalement sur la détection d'artefacts visuels (approche vouée à l'obsolescence)

2. Exploite les limitations physiques et computationnelles inhérentes à toute tentative de simulation en temps réel

3. Rende le coût et la complexité d'une attaque réussie disproportionnés par rapport aux bénéfices potentiels

4. Soit résilient face aux compromissions de dispositifs individuels

5. Puisse s'adapter à différents niveaux de risque (vérification quotidienne vs. opérations à enjeux élevés)

EXPOSÉ DE L'INVENTION

3.1 Objectifs de l'invention

L'invention a pour objectif de proposer une rupture technologique dans le domaine de la vérification d'authenticité physique, en déplaçant le paradigme depuis la "détection d'artefacts ou autres indices et marqueurs de falsification" vers la "validation de cohérence physique multi-sources".

Les objectifs spécifiques sont :

- Rendre la falsification computationnellement impraticable plutôt que simplement difficile à détecter

- Exploiter les lois de la physique (incluant, sans s'y limiter : comportements optiques et propagation lumineuse, réflexions et réfractions, dynamique des fluides (liquides, gaz, fumées, particules), dynamique des solides, interactions mécaniques, comportements inertiels, phénomènes acoustiques, phénomènes thermiques (conduction, convection, rayonnement infrarouge), latences et temps de traitements) comme fondement de la vérification

- Exploiter l'impossibilité pratique de simuler ces phénomènes physiques de manière convaincante en temps réel, sous la contrainte de réaction aux instructions du système - que ces instructions soient destinées aux dispositifs (incluant, sans s'y limiter : affichage de séquences visuelles, émission de signaux) ou aux utilisateurs (incluant, sans s'y limiter : mouvements, positionnements, manipulations d'objets) - et ce sur plusieurs angles de capture simultanés avec une pluralité de capteurs

- Permettre une vérification à plusieurs niveaux de rigueur selon les enjeux (une inscription sur un réseau social ne requiert pas le même niveau de vérification qu'une transaction immobilière ou un acte notarié)

- Offrir une solution pérenne qui ne devienne pas obsolète avec l'amélioration des technologies génératives, et dont les techniques de vérification peuvent être déployées progressivement, renforcées ou combinées au fur et à mesure de l'évolution des capacités des attaquants

3.2 Solution technique proposée

Pour atteindre ces objectifs, l'invention propose un système et procédé utilisant une pluralité de sources de capture (incluant, sans s'y limiter : caméras, microphones, capteurs inertiels, capteurs de profondeur, récepteurs de signaux) réparties sur un ou plusieurs dispositifs, dont les données sont analysées de manière corrélée et synchronisée par une entité de vérification.

Le principe fondamental est le suivant : simuler, générer, synthétiser, ou rendre (render) une scène réelle de manière convaincante sur UN flux vidéo est devenu possible grâce aux avancées en intelligence artificielle générative, inférence neuronale, et techniques de rendu en temps réel. Cependant, simuler, générer ou inférer cette même scène de manière parfaitement cohérente sur PLUSIEURS flux vidéo simultanés, provenant d'angles différents, avec des interactions lumineuses croisées, des réflexions cohérentes, et des contraintes temporelles strictes, dépasse les capacités computationnelles actuelles et

prévisibles à moyen, voire long terme.

L'invention se caractérise par :

- CAPTURE MULTI-SOURCES : Utilisation d'au moins deux sources de capture distinctes fournissant soit des perspectives différentes de la même scène, soit des perceptions de nature différente de cette même scène, soit une combinaison des deux.
  Ces sources peuvent être :
  (a) réparties sur plusieurs dispositifs distincts, indépendants ou organisés selon une architecture de coordination (incluant, sans s'y limiter : configuration maître-esclave, coordinateur-participants, ou toute autre topologie de contrôle),
  (b) intégrées à un dispositif unique (capteurs multiples intégrés, fixes ou mobiles),
  (c) connectées à un dispositif principal via liaison filaire ou sans fil (capteurs internes ou externes, détachables ou non détachables, mobiles ou fixes, motorisés ou non motorisés),
  (d) intégrées à un dispositif auxiliaire ou accessoire, lui-même rattaché à un dispositif principal, ou intégrées à une partie détachable d'un dispositif modulaire ou segmentable (incluant, sans s'y limiter : modules de capture, extensions sensorielles, accessoires avec capteurs intégrés, parties détachables de dispositifs pliables ou modulaires fonctionnant de manière autonome ou semi-autonome),
  (e) réparties sur un ensemble de dispositifs équivalents ou jumelés, commercialisés comme un système unifié, où aucun dispositif n'est désigné comme principal (par exemple : dispositifs jumeaux, appareils symétriques détachables, ou configurations pair-à-pair),
  (f) appartenant à l'utilisateur, à un tiers, ou à disposition publique, incluant sans s'y limiter : dispositifs vestimentaires ou corporels (montres, lunettes, accessoires connectés, implants), capteurs d'infrastructure (caméras de surveillance, capteurs de bâtiment), dispositifs publics ou semi-publics (bornes, terminaux, distributeurs), ou dispositifs mis à disposition temporairement (empruntés, loués, partagés, que ce soit dans le cadre d'un service dédié, d'un partenariat, ou de toute autre circonstance), fixes ou mobiles,
  ou toute combinaison de ces configurations, quel que soit le format, la taille, ou la destination première des dispositifs concernés (incluant, sans s'y limiter : dispositifs avec ou sans écran, vestimentaires, corporels, fixes, mobiles, d'infrastructure, dédiés ou non à la vérification, électroménagers connectés, consoles de jeu, ou tout autre dispositif disposant de capacités de capture).

- RECOUPEMENT SYNCHRONISÉ : Analyse corrélée des flux provenant des différentes sources pour vérifier leur cohérence selon de multiples critères incluant, sans s'y limiter : cohérence géométrique, photométrique, radiométrique, télémetrique, temporelle, acoustique, inertielle, thermique, spectrale, cinématique (mouvements et vitesses), topologique (relations spatiales), comportementale, statistique, électromagnétique (signaux RF, WiFi, Bluetooth), positionnelle, biométrique, entropique, causale (relations cause-effet), et contextuelle.

- DÉFIS PHYSIQUES : Introduction d'éléments de vérification exploitant les lois de la physique, incluant sans s'y limiter :
  * Comportements optiques : propagation lumineuse, réflexions, réfractions, caustiques, interréflexions, sous-diffusion de surface (subsurface scattering), ombres et pénombres, parallaxe
  * Dynamique des fluides : liquides, gaz, fumées, particules, turbulences, effets capillaires, comportements chaotiques
  * Dynamique des solides : déformations, collisions, interactions mécaniques, comportements élastiques
  * Comportements inertiels : accélérations, décélérations, momentum, forces gravitationnelles
  * Phénomènes acoustiques : propagation sonore, réverbération, échos, signatures acoustiques environnementales
  * Phénomènes thermiques : transferts de chaleur (conduction, convection, rayonnement), signatures thermiques
  * Phénomènes électromagnétiques : propagation des signaux RF, WiFi, Bluetooth, variations de champ magnétique

  La simulation correcte de ces phénomènes en temps réel, sur plusieurs angles simultanément, demeure computationnellement prohibitive dans l'état actuel de la technologie.

- VÉRIFICATION PAR CAPTURE CROISÉE : Dans la configuration de base, chaque dispositif peut être dans le champ de capture d'au moins un autre dispositif, confirmant leur co-présence physique dans la même scène. Cette capture mutuelle permet de vérifier que les dispositifs sont effectivement co-localisés et non simulés indépendamment.

- DÉFIS VISUELS ON-SCREEN : L'entité de vérification commande l'affichage de stimuli visuels (incluant, sans s'y limiter : formes géométriques, patterns de couleurs, séquences animées) sur l'écran d'un dispositif, ces stimuli étant capturés par un autre dispositif. Cette technique permet de vérifier :
  * La correspondance entre le stimulus envoyé et le stimulus capturé
  * La cohérence géométrique de la capture (distorsion, angle)
  * La synchronisation temporelle (timing correct)
  * L'authenticité de l'écran (non injection de flux)

  Cette vérification peut être effectuée sans nécessiter de boucle de rétroaction complète (mise en abyme). Les stimuli peuvent également être générés et gérés localement par les dispositifs eux-mêmes.

- BOUCLE DE RÉTROACTION OPTIQUE : Dans certains modes de réalisation, les écrans des dispositifs se "voient" mutuellement à travers leurs caméras, créant un effet de rétroaction visuelle (mise en abyme) dont la simulation fidèle requiert un rendu récursif en temps réel. Il peut également être envisagé d'intégrer une surface réfléchissante dans le processus de vérification, permettant notamment une vérification améliorée avec un seul dispositif : l'écran du dispositif se voyant lui-même dans la surface réfléchissante via la caméra, créant une boucle de rétroaction sans nécessiter de second appareil. La surface réfléchissante présente en outre l'avantage d'être un élément optique physique, avec les implications et avantages associés.
  Cette configuration mono-dispositif avec surface réfléchissante constitue un niveau de vérification accessible lorsque l'utilisateur ne dispose pas d'un second dispositif, d'un lieu public équipé, ou d'un accessoire de vérification dédié.

- ANCRES D'ENTROPIE : Introduction d'éléments physiques à haute entropie (tels que, sans s'y limiter : mouvements de fluides, objets déformables) dont le comportement chaotique est pratiquement impossible à simuler de manière convaincante sur plusieurs angles simultanément.

- TECHNIQUES COMPLÉMENTAIRES : Ensemble de méthodes auxiliaires incluant, sans s'y limiter : vérification par ondes sonores, pièges d'interface utilisateur, stéganographie dynamique, corrélation accélérométrique, et tests de latence.

3.3 Avantages et capacités du multi-source

Le principe de capture multi-source ouvre un large éventail de techniques de vérification, exploitables individuellement ou en combinaison. Ces techniques incluent, sans s'y limiter :

A) TECHNIQUES DE RECOUPEMENT GÉOMÉTRIQUE :
- Vérification de cohérence angulaire entre les perspectives capturées
- Analyse de parallaxe (déplacement différentiel objets proches/lointains)
- Reconstruction 3D implicite à partir des vues multiples
- Vérification de cohérence des dispositions, proportions et dimensions
- Analyse des relations d'occlusion (quel objet cache quel autre)

B) TECHNIQUES DE RECOUPEMENT PHOTOMÉTRIQUE :
- Cohérence des conditions d'éclairage entre les sources
- Vérification de cohérence des ombres et pénombres
- Analyse des reflets et leur cohérence géométrique
- Vérification des caustiques et interréflexions
- Cohérence chromatique entre les captures

C) TECHNIQUES DE RECOUPEMENT TEMPOREL :
- Synchronisation précise des flux capturés
- Corrélation temporelle des événements observés
- Analyse de la cohérence des mouvements entre perspectives
- Vérification des délais et latences

D) TECHNIQUES EXPLOITANT L'AFFICHAGE (ON-SCREEN) :
- Défis visuels commandés par l'entité de vérification
- Patterns géométriques à reconnaissance de forme
- Séquences de couleurs avec vérification de correspondance
- Animations dont le timing et la forme sont vérifiés
- QR codes dynamiques ou motifs visuels encodés

E) TECHNIQUES DE CAPTURE CROISÉE :
- Vérification de co-présence des dispositifs dans la scène
- Un dispositif capturant l'écran d'un autre
- Même flux capturé par plusieurs sources (multi-niveau)
- Validation croisée des flux directs et indirects

F) TECHNIQUES INERTIELLES ET POSITIONNELLES :

- Corrélation des données inertielles (accéléromètre, gyroscope, orientation) avec le mouvement visuel observé
- Cohérence des données GPS/positionnelles entre dispositifs

G) TECHNIQUES ACOUSTIQUES :
- Cohérence de l'empreinte acoustique environnementale entre sources
- Corrélation audio/vidéo (lip-sync multi-angles)
- Analyse des délais de propagation sonore
- Vérification de réverbération cohérente

H) TECHNIQUES ÉLECTROMAGNÉTIQUES :
- Cohérence des signaux RF/WiFi/Bluetooth entre dispositifs
- Comparaison de l'environnement électromagnétique ambiant (tout signal détectable)
- Vérification de cohérence du champ magnétique local
- Corrélation des variations magnétométriques avec les mouvements observés

I) TECHNIQUES D'ENTROPIE ET CHAOS :
- Utilisation d'ancres d'entropie (fluides, objets déformables)
- Exploitation de comportements chaotiques vérifiables
- Patterns imprévisibles mais cohérents entre perspectives

J) TECHNIQUES DE BOUCLE OPTIQUE :
- Mise en abyme : appareils équipés d'écran et/ou caméra, se voyant et/ou se filmant mutuellement, et/ou se filmant eux-mêmes via surface réfléchissante ou par l'intermédiaire de l'affichage d'un autre appareil
- Rétroaction visuelle récursive

Axes de vérification exploitables (incluant, sans s'y limiter) :
- Fidélité de la récursion (correspondance stimulus affiché / capturé)
- Portion visible de la scène dans la boucle (varie selon orientation/position)
- Cohérence géométrique (angles, distorsions, perspectives)
- Cohérence temporelle (délais de propagation dans la boucle)
- Réponse aux défis commandés visibles dans la récursion
- Cohérence photométrique (couleurs, luminosité, reflets)

K) TECHNIQUES BIOMÉTRIQUES MULTI-ANGLES :

Capture et vérification de marqueurs biométriques via le setup multi-source, incluant, sans s'y limiter :
- Cohérence faciale sous plusieurs angles
- Analyse de micro-expressions multi-perspectives
- Cohérence des mouvements corporels
- Empreintes digitales et palmaires (capture visuelle et/ou multi-angle en haute résolution)
- Géométrie de la main (forme, proportions, articulations)
- Morphologie de l'oreille
- Patterns veineux (main, poignet)
- Texture cutanée
- Iris et motifs oculaires (si résolution suffisante)
- Tout autre marqueur biométrique captable visuellement

Utilisation simultanée de capteurs biométriques dédiés :
- Lecture simultanée sur les capteurs des différents dispositifs

(ex: un doigt de chaque main sur le lecteur d'empreinte de chaque appareil), que les données biométriques soient transmises au serveur ou non
- Lecture séquentielle du même doigt sur plusieurs dispositifs, sans coupure du champ visuel (le doigt reste visible durant le passage d'un capteur à l'autre)
- Corrélation temporelle des captures biométriques
- Vérification que les données proviennent du même individu, si applicable (incluant, sans s'y limiter : synchronicité des données de pouls, cohérence des caractéristiques biométriques entre capteurs)

L) TECHNIQUES DE DÉFI COMMANDÉ :
- Instructions de mouvement vérifiables (tourner, pivoter)
- Commandes d'interaction avec objets physiques
- Timing imposé par l'entité de vérification
- Challenges imprévisibles avec réponse attendue

Avantage du second écran pour les instructions :
- En présence d'un second dispositif avec écran, les instructions peuvent être affichées de manière plus précise et détaillée visuellement (voir Figure 3)
- Guidage visuel en temps réel (flèches, animations, zones à cibler)
- Feedback immédiat sur l'exécution des instructions
- Précision accrue par rapport aux instructions textuelles ou audio seules

Ces techniques peuvent être combinées selon les enjeux de la vérification, permettant un gradient de rigueur adapté au contexte.

3.4 Avantages de l'invention

- RÉSILIENCE TEMPORELLE : Contrairement aux détecteurs d'artefacts, le système ne devient pas obsolète avec l'amélioration des générateurs, car il exploite des limitations physiques fondamentales.

- COÛT ASYMÉTRIQUE : Le coût computationnel pour falsifier le système est exponentiellement plus élevé que le coût pour le vérifier, inversant le déséquilibre actuel.

- AVANTAGE ASYMÉTRIQUE TEMPOREL : L'attaquant doit simuler en temps réel (contrainte forte de latence pour maintenir l'illusion), tandis que le serveur/vérificateur peut analyser les données a posteriori, sans contrainte de temps réel. Pour les opérations à enjeux élevés, la validation peut être asynchrone, permettant des analyses plus profondes (reconstruction 3D, corrélation fine des micro-mouvements, vérification de cohérence exhaustive). Cette asymétrie temporelle constitue un avantage structurel majeur du système.

- ADAPTABILITÉ : Le système peut opérer à différents niveaux de rigueur, depuis une vérification basique (deux caméras, tests simples) jusqu'à une vérification maximale (grand nombre de dispositifs, intégration de tous les tests disponibles dans une seule session).

- RÉSISTANCE AUX COMPROMISSIONS : La compromission d'un, voire de tous les dispositifs, ne suffit pas nécessairement à tromper le système, car la

cohérence multi-sources et la fidélité de la scène doivent être maintenues.

- INDÉPENDANCE DES ALGORITHMES : Le procédé ne dépend pas d'un algorithme de détection spécifique qui pourrait être contourné ; il repose sur une combinaison de facteurs, ainsi que sur des principes physiques universels.

- EFFICACITÉ ÉCONOMIQUE ET PRIVACY : Certaines techniques de vérification (incluant, sans
s'y limiter : pièges algorithmiques, tests à résultat attendu, vérifications statistiques) offrent un rapport coût/efficacité particulièrement favorable au défenseur, permettant une protection robuste avec des ressources modérées. La combinaison de ces techniques peut constituer une première ligne de défense efficace et accessible. Ces mêmes techniques permettent également, lorsque souhaité, de réduire l'exposition de données sensibles en effectuant certaines vérifications sur la base de signatures, hashs, métadonnées, ou résultats de tests plutôt que sur les flux bruts complets, limitant ainsi le volume de données personnelles transmises ou stockées.

- SYNERGIE AVEC ÉVOLUTIONS HARDWARE : Le protocole bénéficiera des améliorations futures des dispositifs (incluant, sans s'y limiter : attestation hardware de l'origine des flux, signatures cryptographiques au niveau capteur, patterns d'image certifiés, chaîne de confiance depuis le capteur). Ces évolutions renforceront le protocole sans le remplacer ; celui-ci reste pleinement efficace avec le matériel actuel, sans dépendance envers les fabricants ou opérateurs contrôlant l'authentification hardware - garantissant ainsi une autonomie de fonctionnement.

- AVANTAGE STRUCTUREL DU DÉFENSEUR : La centralisation des ressources de vérification (data science, R&D, adaptation continue des tests) permet au défenseur d'évoluer plus rapidement que les attaquants, qui doivent reverse-engineer chaque mise à jour sans accès aux données statistiques globales. Chaque nouveau facteur de vérification multiplie le coût d'attaque.

DESCRIPTION DÉTAILLÉE

4.1 Architecture générale

Le système selon l'invention comprend :

a) AU MOINS DEUX SOURCES DE CAPTURE, DE NATURE ET/OU DE PERSPECTIVE DIFFÉRENTE :

Ces sources peuvent être configurées selon l'une des modalités suivantes, ou toute combinaison de celles-ci :

- CONFIGURATION MULTI-DISPOSITIFS : Deux ou plusieurs dispositifs physiquement distincts, incluant, sans s'y limiter :
  * Dispositifs personnels de l'utilisateur (téléphones, tablettes, ordinateurs avec webcam, montres connectées, lunettes connectées)
  * Dispositifs tiers, dédiés ou non dédiés à la vérification
  * Dispositifs publics ou semi-publics (bornes interactives, terminaux de paiement, distributeurs automatiques équipés de caméras, guichets automatiques bancaires, écrans publicitaires interactifs, kiosques

d'information, automates de vente)
  * Dispositifs d'infrastructure existante (caméras de surveillance, systèmes de vidéoconférence, équipements de points de vente, caméras de contrôle d'accès)
  * Dispositifs mis à disposition par un opérateur, partenaire commercial, établissement public ou privé, ou tout autre tiers (de manière permanente, temporaire, ou ponctuelle)
  * Tout appareil équipé d'au moins une source de capture et capable de communiquer avec le système de vérification, ou autrement capable de servir de point de référence pour la vérification (incluant, sans s'y limiter : dispositifs affichant des valeurs dynamiques validables par secret cryptographique partagé), indépendamment de sa fonction première ou de son propriétaire
- CONFIGURATION MONO-DISPOSITIF INTÉGRÉE : Un dispositif unique équipé de multiples capteurs intégrés (exemple : caméra frontale et caméra arrière d'un téléphone, ou multiples caméras arrière)
- CONFIGURATION AVEC CAPTEURS EXTERNES : Un dispositif principal connecté à un ou plusieurs capteurs externes via liaison filaire ou sans fil (exemple : téléphone connecté à une caméra externe, drone, capteur détachable, ou périphérique mobile)
- Les sources de données, permettant de caractériser des grandeurs physiques et/ou l'état de la scène ou situation vérifiée, incluent, sans s'y limiter :
  * Capteurs de grandeurs physiques (images, sons, profondeur, température, pression, accélération, orientation, luminosité, proximité)
  * Capteurs télémétriques (lidar, ToF, radar, ultrasons)
  * Récepteurs de signaux électromagnétiques (antennes radio, WiFi, Bluetooth, NFC, GSM/cellulaire, GPS, signaux radio locaux)
  * Modules cryptographiques ou de sécurité (puces sécurisées, éléments de réponse cryptographique, générateurs de tokens)
  * Données environnementales captées (stations radio détectées, réseaux WiFi visibles, tours cellulaires à proximité, balises Bluetooth)
  * Toute donnée ou métadonnée reflétant l'état, la configuration, ou les conditions de la scène, de l'environnement, ou de la situation vérifiée
  * Tout autre moyen de capture, réception, ou génération de données pouvant être corrélées pour établir l'authenticité

La présente invention couvre également les configurations où les sources de capture multiples sont intégrées à un même produit commercial sous forme de modules détachables, périphériques embarqués, extensions du dispositif principal, ou composants d'un écosystème de produit unifié, indépendamment de leur mode de connexion (filaire, sans fil, ou interne) ou de leur commercialisation comme produit unique ou ensemble de produits séparés. L'invention s'applique dès lors qu'au moins deux perspectives distinctes d'une même scène sont capturées et analysées de manière corrélée, quelle que soit la configuration matérielle utilisée.

Note : Dans le cadre du protocole, tout dispositif peut assumer le rôle de sujet requérant vérification, d'auxiliaire participant à la vérification d'un autre sujet, ou les deux simultanément. Les dispositifs peuvent recevoir toute instruction et assumer tout rôle nécessaire au processus de vérification, selon les besoins et la configuration de la session.

b) UNE ENTITÉ DE VÉRIFICATION :
Unité ou ensemble d'unités de traitement recevant les flux de données des sources de capture et effectuant l'analyse corrélée. Cette entité peut prendre diverses formes, incluant, sans s'y limiter :

ARCHITECTURES CENTRALISÉES (niveau de sécurité maximal) :
- Un serveur distant contrôlé par le vérificateur
- Une infrastructure cloud contrôlée par le vérificateur
- Une instance locale dédiée
- Un système distribué sous contrôle unifié

ARCHITECTURES DÉCENTRALISÉES OU HYBRIDES :
- Un réseau pair-à-pair (peer-to-peer) de nœuds de vérification
- Des ressources de calcul externalisées (incluant, sans s'y limiter, des réseaux de calcul distribué, des services de computation à la demande, ou des ressources louées ou empruntées sur des appareils tiers)
- Un dispositif public ou semi-public servant de point d'ancrage de confiance (incluant, sans s'y limiter : borne, terminal, distributeur automatique) effectuant tout ou partie de la vérification localement
- Une vérification répartie entre plusieurs dispositifs participants, avec ou sans serveur central

ARCHITECTURES HORS-LIGNE OU AUTONOMES [MODES DÉGRADÉS] :
- Vérification effectuée localement sur les dispositifs eux-mêmes, avec synchronisation ultérieure optionnelle
- Vérification pair-à-pair directe entre dispositifs sans serveur
- Dispositifs effectuant tout ou partie de la vérification, qu'ils soient de confiance ou non, pré-autorisés ou non, incluant sans s'y limiter : dispositifs désignés, dispositifs sélectionnés arbitrairement, dispositifs tiers actuellement connectés, ou tout dispositif recruté dynamiquement

IMPORTANT - STATUT DE CES ARCHITECTURES :
Les architectures hors-ligne et autonomes décrites ci-dessus constituent des MODES DÉGRADÉS ou de REPLI (fallback). Elles sont décrites pour assurer la flexibilité opérationnelle du système, mais NE SONT PAS revendiquées comme innovantes en elles-mêmes lorsqu'elles impliquent un mono-dispositif sans dépendance externe. Une vérification purement locale sur un appareil unique relève de l'état de l'art existant (cf. section 6.1 - EXCLUSION). Toutefois, même en mode dégradé, les TECHNIQUES SPÉCIFIQUES décrites dans la présente demande (rétroaction visuelle, ancres d'entropie, etc.) restent des innovations protégeables indépendamment.

Note : Le niveau de sécurité maximal est atteint avec une architecture centralisée où le serveur de vérification est contrôlé et sécurisé par l'opérateur du service. Les architectures alternatives offrent des compromis entre accessibilité, coût, et niveau de confiance, adaptés selon les enjeux de la vérification concernée et les moyens à disposition.

Note : Les configurations pair-à-pair peuvent apporter une valeur de vérification supplémentaire dans le cas de vérifications de groupe (incluant, sans s'y limiter : équipes, événements, activités collectives). Dans ce contexte, la corrélation de multiples dispositifs (ex: 20+ capteurs

pour un groupe de 20 personnes) renforce la vérification, et les connexions pair-à-pair entre dispositifs co-localisés peuvent ajouter un facteur de confiance lié à leur proximité physique. Toutefois, les méthodes pair-à-pair passant par un réseau relayé (avec antenne extérieure aux appareils) offrent moins de garanties que les communications de proximité locale (incluant, sans s'y limiter : Bluetooth, NFC, WiFi Direct, ultrasons).

INFRASTRUCTURE DE SERVEURS RELAIS (optimisation de latence et triangulation) : Le système peut être doté de serveurs relais répartis géographiquement, a minima dans les principaux centres urbains et zones de population, servant de points d'entrée au réseau de vérification. Ces relais permettent :

- Latence minimale : Chaque utilisateur communique avec le relais le plus proche, réduisant le délai de transmission au minimum physiquement possible pour sa localisation.

- Authentification du ping minimal : Le relais authentifie et horodate l'arrivée des données, établissant une preuve de latence minimale attendue selon la distance géographique déclarée.

- Triangulation par différentiel de latence : En effectuant des pings vers plusieurs serveurs relais simultanément (ou en mesurant les temps de réponse depuis plusieurs relais), le système peut inférer la position approximative de l'utilisateur. La comparaison des latences mesurées vers chaque relais permet de confirmer ou infirmer la localisation déclarée.

- Corrélation avec données tierces : La position inférée peut être comparée avec d'autres sources de données, incluant, sans s'y limiter : données GPS déclarées, géolocalisation de l'adresse IP (pays, région, ville associés à l'IP par les bases de données de géolocalisation IP), données d'autres utilisateurs dans la même zone géographique (cohérence environnementale de groupe).

  Exemple : si le serveur relais est à Paris, que l'utilisateur a une adresse IP géolocalisée à Paris, mais présente une latence de 400ms (incompatible avec une connexion locale), cela indique l'utilisation probable d'un VPN ou d'un proxy. Le système peut alors demander à l'utilisateur de désactiver ces outils pour poursuivre la vérification.

Cette infrastructure n'est pas nécessairement propre au présent protocole et peut s'appuyer sur des infrastructures existantes ou partagées.

c) DES MOYENS DE COMMUNICATION :
Interfaces permettant la transmission des données, de manière filaire ou non filaire, directe ou indirecte, entre les sources de capture et l'entité de vérification, incluant, sans s'y limiter :
- Protocoles standards : Wi-Fi, réseaux cellulaires (4G, 5G, et générations futures), Bluetooth, NFC, Zigbee, LoRa, satellite
- Protocoles propriétaires ou personnalisés (custom)
- Communications filaires (USB, Ethernet, série)
- Tout autre protocole de communication existant ou à venir

Les données transmises peuvent également inclure des informations sur l'environnement radio lui-même, telles que, sans s'y limiter : signaux radio détectés (incluant, sans s'y limiter : stations FM/AM, fréquences, puissances), réseaux visibles, identifiants de tours cellulaires, signatures électromagnétiques ambiantes, ou toute autre donnée captable relative aux signaux environnants.

d) DES MOYENS D'ÉMISSION COMMANDABLES :
Dispositifs permettant d'émettre des signaux ou stimuli commandés par l'entité de vérification, incluant, sans s'y limiter :

* Émissions visuelles : écrans affichant des contenus (séquences de couleurs, motifs visuels, éléments graphiques, codes, flux vidéo, texte statique ou dynamique, instructions), LEDs, flashs, projecteurs, lasers
* Émissions sonores : haut-parleurs émettant des sons audibles ou ultrasons, signaux acoustiques codés, séquences audio
* Émissions électromagnétiques : signaux radio, Bluetooth, NFC, WiFi, ou tout autre signal électromagnétique commandable
* Émissions physiques/mécaniques : vibreurs, moteurs, actionneurs, contrôle kinétique, déplacement de composants mobiles
* Émissions thermiques : éléments chauffants ou refroidissants commandables
* Émissions futures ou spécialisées : champs magnétiques directionnels, faisceaux d'énergie, transmission d'énergie sans fil, drones ou éléments mobiles associés au dispositif, ou toute autre forme d'émission physique ou énergétique commandable

Ces moyens d'émission permettent de créer des stimuli vérifiables par les capteurs des autres dispositifs participants à la vérification.

Note sur l'étendue des commandes de l'entité de vérification :
L'entité de vérification peut envoyer tout type de commande à tout dispositif participant au processus de vérification, incluant, sans s'y limiter :
- Commandes d'émission : déclencher des émissions visuelles, sonores, électromagnétiques, ou physiques (tel que décrit ci-dessus)
- Commandes de capture : activer/désactiver des flux vidéo ou audio, prendre des photos, déclencher des enregistrements, alterner entre caméras (front/back, switching rapide ou séquentiel), ajuster les paramètres de capture (résolution, framerate, exposition)
- Commandes de transmission : requérir l'envoi de données spécifiques de capteurs (inertiels, positionnels, environnementaux), de métadonnées, de données système, de données d'utilisation, ou de toute autre donnée accessible sur le dispositif
- Commandes d'affichage : contrôler ce qui est affiché sur l'écran, superposer des éléments visuels, afficher des instructions
- Commandes de configuration : modifier les paramètres du dispositif pour les besoins de la vérification
- Toute autre commande nécessaire au bon déroulement de la vérification

Le timing, la séquence, et la nature des commandes sont déterminés par l'entité de vérification selon les besoins du test, de manière prévisible

ou imprévisible pour l'utilisateur et tout attaquant potentiel. Cette flexibilité totale permet d'adapter les défis en temps réel et de rendre toute tentative de simulation ou de prédiction prohibitivement complexe.

e) OPTIONNELLEMENT, DES CAPTEURS ET DONNÉES COMPLÉMENTAIRES :
Capteurs, accessoires, et sources de données supplémentaires pouvant enrichir le processus de vérification, incluant, sans s'y limiter :

* Capteurs de grandeurs physiques : accéléromètres, gyroscopes, capteurs de lumière ambiante, microphones, capteurs de profondeur, lidars, capteurs temps de vol (ToF), radars, magnétomètres, baromètres
* Capteurs environnementaux : température, humidité, pression atmosphérique, qualité de l'air, altitude
* Capteurs de positionnement : GPS, GNSS, boussole, altimètre
* Données système et contextuelles : état du dispositif, horodatage, identifiants matériels, métadonnées de configuration
* Accessoires et périphériques connectés : capteurs externes, objets connectés (IoT), modules complémentaires
* Toute autre source de données ou capteur pouvant contribuer à l'établissement de l'authenticité de la scène ou situation vérifiée.

4.2 Configurations de vérification

L'invention prévoit plusieurs configurations de vérification, adaptées aux enjeux et aux contraintes pratiques.

Note préliminaire : Les configurations décrites ci-dessous sont présentées à titre indicatif et non hiérarchique. Elles peuvent être librement combinées, modulées, ou adaptées selon les enjeux de sécurité, le matériel disponible, et les contraintes pratiques. Cette liste n'est pas exhaustive ; toute configuration permettant une vérification multi-perspectives ou multi-modalités est couverte par la présente invention, qu'elle soit décrite explicitement ci-dessous ou non. La combinaison de plusieurs configurations est recommandée pour atteindre un niveau de confiance élevé.

A) CONFIGURATION MONO-DISPOSITIF

Utilisation d'un seul dispositif, selon l'une des configurations suivantes, ou toute combinaison de celles-ci :

a) Multi-caméras intégrées : dispositif équipé de plusieurs caméras (exemple : téléphone avec caméras avant et arrière). L'analyse porte sur la cohérence angulaire entre les perspectives, et sur la corrélation avec les données des capteurs inertiels lors des mouvements.

Exploitation de l'écran comme source lumineuse : l'écran du dispositif, orienté vers l'avant, peut émettre des patterns lumineux commandés (séquences de couleurs, variations d'intensité, formes animées). Ces émissions lumineuses produisent simultanément :
- Un éclairage de la scène située derrière l'utilisateur (capturable par la caméra arrière)
- Des réflexions sur le visage et les yeux de l'utilisateur (capturables

par la caméra frontale)
La corrélation entre ces deux effets (éclairage scène + reflets visage) constitue une double vérification difficile à simuler de manière cohérente. Le flash du dispositif peut être utilisé de manière similaire, créant des ombres analysables sur la scène arrière et une illumination du visage.

b) Mono-caméra avec retour visuel : utilisation d'une seule caméra en combinaison avec un dispositif de retour visuel, permettant de créer une boucle de rétroaction optique (effet abyme/mise en abyme) où l'écran du dispositif se voit lui-même.

Les dispositifs de retour visuel incluent, sans s'y limiter :
- Surfaces réfléchissantes (incluant, sans s'y limiter : surface réfléchissante de poche, murale, publique, ou toute autre surface réfléchissante disponible)
- Écrans numériques avec retour visuel : tout appareil non appairé affichant un flux vidéo en retour (écran public, téléviseur, moniteur, tablette, ou autre dispositif d'affichage)

B) CONFIGURATION MULTI-DISPOSITIFS

Utilisation de deux dispositifs indépendants ou plus. L'appairage s'effectue par lecture d'un motif visuel encodé (incluant, sans s'y limiter : QR code, code-barres, motif graphique - voir Figure 2) et/ou par communication sans fil de proximité (incluant, sans s'y limiter : Bluetooth, NFC, WiFi Direct). Les dispositifs exécutent des commandes émises par l'entité de vérification (incluant, sans s'y limiter : affichage de séquences visuelles, émissions sonores, flashs lumineux, émissions radio, ou toute autre forme d'émission commandable), et chaque capteur observe la scène, incluant ou non l'autre dispositif dans son champ de perception.

Configuration avec boucle optique : les dispositifs peuvent être positionnés de sorte que chaque caméra puisse observer l'écran de l'autre dispositif. Ceci crée une boucle de rétroaction visuelle (effet de réflexion infinie ou mise en abyme - voir Figure 3) dont les caractéristiques temporelles et géométriques sont analysées.

C) TECHNIQUES COMPLÉMENTAIRES

Les configurations ci-dessus peuvent être enrichies par l'une ou plusieurs des techniques suivantes, applicables en mono-dispositif comme en multi-dispositifs, sans s'y limiter :

c.1) Ancres d'entropie : introduction dans la scène d'un élément physique à haute entropie (tel que, sans s'y limiter : récipient contenant un liquide, tissu, objet déformable, fumée, particules). Les mouvements chaotiques de cet élément doivent être cohérents sur tous les angles de capture.

c.2) Ancrage cryptographique : utilisation d'un objet d'authentification spécialisé (token physique, puce sécurisée, objet à réponse cryptographique) interagissant avec le ou les dispositifs.

c.3) Stimuli commandés et corrélations : vérifications sonores (temps de propagation acoustique), corrélations accélérométriques (cohérence des données inertielles entre dispositifs), et tests de latence (mesure des délais de transmission et réponse).

c.4) Accessoires de vérification : tout objet ou source présent dans l'environnement de l'utilisateur peut servir d'accessoire, incluant sans s'y limiter :

- Objets émetteurs de son : carte musicale, jouet sonore, instrument, haut-parleur, ou tout objet produisant un son analysable
- Objets émetteurs de lumière : lampe, bougie, écran secondaire, LED, indicateurs lumineux, ou tout objet produisant une lumière modulable
- Éléments d'environnement : éclairage de la pièce, robinet (flux d'eau contrôlable), ventilateur, tout élément contrôlable par l'utilisateur
- Objets modulables : tout objet pouvant changer de forme, de manière autonome ou par manipulation (jouet articulé, objet pliable, mécanisme mobile, etc.)
- Objets identifiables : tout objet avec caractéristiques visuelles distinctives vérifiables sous plusieurs angles

Tout élément de l'environnement susceptible de produire un stimulus vérifiable (visuel, sonore, ou autre) peut constituer un accessoire valide pour la vérification multi-capteurs.

4.3 Procédé de vérification - Principes généraux

Le procédé selon l'invention repose sur les principes fondamentaux suivants :

A) ACQUISITION MULTI-PERSPECTIVES :
Capture simultanée ou quasi-simultanée de données depuis au moins deux sources de capture distinctes, permettant d'obtenir des perspectives différentes et/ou des modalités de perception différentes d'une même scène ou situation.

B) TRANSMISSION ET SYNCHRONISATION :
Communication des données capturées vers l'entité de vérification, avec synchronisation temporelle permettant l'analyse corrélée.

C) ANALYSE CORRÉLÉE :
Traitement des données multi-sources pour vérifier leur cohérence selon un ou plusieurs critères (incluant, sans s'y limiter : cohérence géométrique, photométrique, radiométrique, télémetrique, temporelle, acoustique, inertielle, thermique, spectrale, cinématique, topologique, comportementale, statistique).

D) DÉTERMINATION D'AUTHENTICITÉ :
Sur la base de l'analyse corrélée, détermination de l'authenticité de la scène, du sujet, ou de la situation vérifiée, avec un niveau de confiance associé.

4.3.1 Techniques de vérification - Présentation générale

L'invention couvre l'utilisation, individuelle ou en combinaison, de techniques de vérification incluant, sans s'y limiter :

a) TECHNIQUES D'ÉTABLISSEMENT DE SESSION :
Méthodes permettant d'établir une session de vérification entre les sources de capture et l'entité de vérification, incluant, sans s'y limiter : appairage par motif visuel encodé, appairage par communication sans fil de proximité, identification automatique (incluant, sans s'y limiter : corrélation géopositionnelle, corrélation de l'environnement radio, perception mutuelle des appareils via signaux radio/Bluetooth), ou toute autre méthode ayant pour but d'associer ou d'identifier les appareils comme étant destinés à participer dans une ou plusieurs sessions ou procédures de vérification, ou eux-mêmes requérant vérification.

b) TECHNIQUES DE CALIBRATION :
Méthodes permettant de caractériser les propriétés des sources de capture et des moyens d'émission, incluant, sans s'y limiter : caractérisation colorimétrique, mesure de latence de base, vérification de communication, établissement de références, ou toute autre caractérisation utile à la vérification.

La calibration peut inclure, sans s'y limiter, une évaluation des capacités et limitations de chaque dispositif participant (incluant, sans s'y limiter : résolution, latence de capture, qualité des capteurs, stabilité temporelle, ou toute autre propriété mesurable), permettant à l'entité de vérification d'adapter dynamiquement les paramètres de test aux capacités du dispositif le moins performant, ou de moduler les tests de toute autre manière.

La calibration peut également établir une synchronisation temporelle relative entre dispositifs par déclenchement d'événements physiques observables (incluant, sans s'y limiter : flash lumineux, signal sonore, changement d'affichage sur écran, variation de signal radio, ou tout autre stimulus perceptible par les capteurs), permettant de référencer les flux capturés à un instant commun sans dépendre de la synchronisation des horloges système des dispositifs, ou par toute autre méthode de synchronisation temporelle.

Ces techniques de calibration sont données à titre illustratif ; toute autre méthode de calibration permettant de caractériser, synchroniser, ou adapter le système aux conditions réelles est couverte par la présente invention.

c) TECHNIQUES DE STIMULATION ET EXPLOITATION DES LIMITATIONS DE RENDU :
Méthodes où l'entité de vérification commande l'émission de stimuli (incluant, sans s'y limiter : séquences visuelles, signaux sonores, émissions électromagnétiques, commandes physiques) et vérifie leur effet sur la scène capturée par les sources de capture.

Ces techniques peuvent spécifiquement cibler des phénomènes physiques particulièrement coûteux à simuler, incluant, sans s'y limiter :
- Caustiques (réfraction de lumière à travers des objets transparents)
- Dynamique des fluides
- Sous-diffusion de surface (subsurface scattering) sur la peau

- Réflexions multiples (interréflexions)

Les algorithmes de vérification peuvent être envoyés dynamiquement par l'entité de vérification, rendant leur reverse-engineering par un attaquant impraticable. Les tests eux-mêmes peuvent varier d'une session à l'autre (diversité algorithmique dynamique).

d) TECHNIQUES DE BOUCLE DE RÉTROACTION :
Méthodes exploitant le fait qu'une source de capture observe le moyen d'émission d'un autre dispositif (ou du même dispositif via surface réfléchissante), créant des effets de rétroaction analysables (mise en abyme, récursion optique).

e) TECHNIQUES D'ANCRAGE ENTROPIQUE :
Méthodes utilisant des éléments physiques à comportement chaotique, imprévisible, ou hautement entropique (incluant, sans s'y limiter : fluides, objets déformables, particules) dont la cohérence multi-perspectives est vérifiée.

f) TECHNIQUES DE CORRÉLATION INERTIELLE :
Méthodes comparant les données de capteurs inertiels (incluant, sans s'y limiter : accéléromètres, gyroscopes) avec les mouvements inférés à partir des captures.

L'inférence de mouvement peut être effectuée à partir de multiples sources de données, incluant, sans s'y limiter : changements de perspective visuels, parallaxe, transformations géométriques, variations acoustiques, variations de signaux radio, décalages temporels inter-capteurs.

g) TECHNIQUES DE VÉRIFICATION DE LATENCE :
Méthodes mesurant et analysant les délais de transmission et de réponse, incluant, sans s'y limiter : requêtes prioritaires basse latence (par exemple, sans s'y limiter : tolérance d'un délai sur le flux vidéo principal, mais requête ponctuelle d'une frame ou fraction de frame/image de la scène, envoyée en priorité, potentiellement via connexion ou canal différent, avec vérification de cohérence par le serveur a posteriori), comparaison géographique des latences, détection de délais anormaux indicatifs de traitement intermédiaire.

Le système peut mesurer les latences de différentes opérations et comparer ces mesures entre elles et aux valeurs attendues. Un système de simulation introduirait des latences spécifiques (temps de rendu) qui ne seraient pas présentes dans une capture authentique.

h) TECHNIQUES DE VÉRIFICATION ACOUSTIQUE :
Méthodes utilisant la propagation sonore pour vérifier les distances et positions physiques entre dispositifs ou éléments de la scène.

Les dispositifs peuvent émettre des signaux sonores (audibles ou ultrasonores). Les microphones des autres dispositifs captent ces signaux. Le temps de propagation permet de calculer les distances

physiques entre dispositifs et de vérifier leur cohérence avec les observations visuelles.

Techniques complémentaires incluant, sans s'y limiter :
- Analyse des réponses vocales de l'utilisateur (parole, instructions verbales demandées)
- Calcul des différences de distance par temps de propagation entre plusieurs microphones
- Cohérence entre la scène visuelle et les sons émis par la voix et les actions de l'utilisateur (lip-sync, bruits d'interaction)
- Traitement adapté selon les caractéristiques connues des appareils utilisés (modèle de microphone, réponse en fréquence, sensibilité)

i) TECHNIQUES DE PIÉGEAGE ET STÉGANOGRAPHIE :
Méthodes où le résultat attendu d'un test est connu uniquement de l'entité de vérification, permettant de détecter des réponses simulées ou falsifiées.

Exemples d'application, sans s'y limiter :
- Pièges d'interface (UI Traps) : l'entité de vérification peut envoyer des éléments d'interface dont le comportement attendu est volontairement différent de ce qu'un système de détection local pourrait prédire. Par exemple, un algorithme de détection de couleur local pourrait être volontairement mis en échec par l'envoi d'une couleur proche de celle d'un élément de la scène, et l'entité de vérification s'attend à ce que cette détection échoue. Un attaquant simulant les réponses, sauf analyse poussée, ne saurait pas quelles détections doivent échouer, ni dans quelle proportion.
- Stéganographie dynamique : des informations cachées (non visibles à l'œil nu mais détectables par analyse fine des flux) peuvent être injectées dans les contenus affichés. La présence ou l'absence de ces éléments dans les captures reçues permet une vérification supplémentaire.

j) TECHNIQUES DE VÉRIFICATION MULTI-MODALE ET TÉLÉMETRIQUE :
Méthodes combinant des données de nature différente (incluant, sans s'y limiter : visuel + lidar, visuel + acoustique, visuel + thermique) pour vérification croisée.

L'invention peut exploiter des techniques d'imagerie existantes, incluant, sans s'y limiter : imagerie stéréoscopique, vision 3D, reconstruction de profondeur, photogrammétrie. Ces techniques d'imagerie, connues en elles-mêmes, sont utilisées dans le cadre de l'invention non pas pour leur finalité originale (reconstruction tridimensionnelle, mesure de distance), mais comme moyens de vérification de cohérence multi-perspectives au service de la détermination d'authenticité.

Les capteurs de distance (incluant, sans s'y limiter : temps de vol / ToF, lidar, radar, ultrasons) peuvent être utilisés pour vérifier la cohérence des mesures de profondeur et de distance avec les observations visuelles et les données des autres capteurs. L'analyse corrélée inclut la vérification télémetrique.

4.3.2 Exemple de flux de vérification (mode de réalisation indicatif)

À titre d'exemple non limitatif, un flux de vérification peut comprendre les phases suivantes. Ces phases sont présentées à titre indicatif et peuvent être omises, réordonnées, combinées, répétées, ou adaptées selon les besoins de la vérification :

PHASE D'INITIATION :
Établissement d'une session de vérification, génération d'identifiants, appairage éventuel des dispositifs participants (voir Figure 2).

PHASE DE CALIBRATION (optionnelle) :
Caractérisation des propriétés des dispositifs, de l'environnement, et du contexte situationnel ; établissement de références (incluant, sans s'y limiter : références colorimétriques, acoustiques, lumineuses, électromagnétiques, géographiques) ; mesure des latences de base.

PHASE DE DÉFIS :
Exécution d'un ou plusieurs défis de vérification sélectionnés selon le niveau de sécurité requis . Ces défis exploitent une ou plusieurs des techniques listées ci-dessus.

PHASE D'ANALYSE :
Traitement corrélé des données reçues utilisant des méthodes computationnelles (incluant, sans s'y limiter : apprentissage automatique, vision par ordinateur, analyse de cohérence, modèles physiques).

PHASE DE DÉCISION :
Détermination de l'authenticité avec niveau de confiance associé. Cette phase peut être différée si l'entité de vérification nécessite un temps supplémentaire pour traiter les données (analyse a posteriori).

MODES DE RÉALISATION

Les modes de réalisation suivants sont présentés à titre d'exemples non limitatifs, destinés à illustrer certaines applications possibles de l'invention. Ces exemples ne sauraient restreindre la portée des revendications, qui couvrent toute mise en œuvre des principes et techniques décrits dans la présente demande, indépendamment du domaine d'application, de la configuration matérielle, ou du contexte d'utilisation.

5.1 Premier mode - Ouverture de compte bancaire

Un utilisateur souhaite ouvrir un compte bancaire en ligne. Le service bancaire requiert une vérification d'identité renforcée.

1. L'utilisateur démarre le processus sur son téléphone mobile.
2. Après avoir fourni ses informations et photographié sa pièce d'identité, l'application lui demande de compléter une vérification de présence.
3. L'application affiche un motif visuel encodé et demande à l'utilisateur d'accéder au site de vérification sur un second dispositif (par exemple son laptop ou un PC public).

4. L'utilisateur scanne le motif (ou appaire via communication sans fil de proximité), les dispositifs sont appairés (voir Figure 2).
5. La vérification multi-dispositifs s'engage : l'utilisateur positionne son téléphone face à la webcam, créant une boucle optique.
6. Des séquences de couleurs sont affichées, les réflexions sur le visage de l'utilisateur sont analysées depuis les deux angles.
7. La vérification réussit, le compte est ouvert.

5.2 Deuxième mode - Transaction à haut risque

Un utilisateur souhaite effectuer un virement bancaire d'un montant significatif depuis un lieu inhabituel.

1. La banque déclenche une vérification de niveau élevé.
2. L'utilisateur utilise deux dispositifs comme précédemment.
3. En plus des tests standards, l'application demande à l'utilisateur de présenter une bouteille d'eau partiellement remplie et de la secouer légèrement.
4. Les mouvements du liquide sont capturés sous deux angles et analysés pour leur cohérence physique.
5. La transaction est autorisée.

5.3 Troisième mode - Mono-dispositif

Pour des vérifications quotidiennes à moindre enjeu, un seul dispositif disposant de caméras multiples est utilisé.

1. L'utilisateur tient son téléphone et active la vérification.
2. Le téléphone utilise simultanément les caméras avant et arrière.
3. L'utilisateur pivote le dispositif et/ou pivote sur lui-même selon les instructions, permettant aux deux caméras de capturer la scène sous différents angles au fil du mouvement.
4. Le serveur vérifie la cohérence angulaire entre les deux perspectives, la corrélation avec les données accélérométriques, et la cohérence temporelle des captures durant le mouvement.
5. La vérification réussit.

5.4 Quatrième mode - État des lieux immobilier

Un propriétaire et un locataire souhaitent réaliser un état des lieux de sortie à distance, chacun étant dans un lieu différent.

1. Le locataire se rend dans l'appartement avec deux dispositifs (deux téléphones, ou un téléphone et une tablette).
2. Il démarre le processus de vérification et appaire les deux dispositifs.
3. Le propriétaire rejoint la session à distance et peut observer les flux vidéo en temps réel.
4. Le locataire parcourt l'appartement en tenant les deux dispositifs, filmant chaque pièce et élément sous plusieurs angles simultanément.
5. Le serveur vérifie continuellement la cohérence géométrique et temporelle des captures multi-angles, garantissant qu'il s'agit d'images réelles et non de vidéos préenregistrées ou manipulées.

6. Pour les éléments nécessitant une attention particulière (état d'un mur, fonctionnement d'un équipement), le locataire rapproche les dispositifs pour une capture détaillée multi-perspectives.
7. Le serveur génère un rapport horodaté certifiant l'authenticité des captures, utilisable comme preuve juridique.

Variante mono-dispositif : L'état des lieux peut également être réalisé avec un seul dispositif équipé de caméras multiples (avant et arrière). Le locataire pivote sur lui-même et déplace le dispositif selon les instructions, permettant aux deux caméras de capturer l'espace sous différents angles. Le recoupement des données et la corrélation avec les capteurs inertiels permettent une vérification d'authenticité, dans une mesure adaptée aux enjeux concernés.

Pour renforcer la vérification mono-dispositif, le système peut exploiter les éléments présents dans le lieu lui-même : par exemple, le locataire peut être invité à se positionner face au miroir de la salle de bain, créant une boucle de rétroaction optique où l'écran du dispositif se voit dans le miroir via la caméra. Cette configuration immersive permet d'effectuer des tests de vérification renforcés sans nécessiter de second appareil, en utilisant l'infrastructure existante du lieu.

5.5 Cinquième mode - Vérification d'objet de valeur

Une compagnie d'assurance souhaite vérifier l'état d'un objet assuré (bijou, oeuvre d'art, instrument de musique) suite à une déclaration.

1. L'assuré utilise deux dispositifs pour capturer l'objet sous plusieurs angles simultanément.
2. Le serveur vérifie la cohérence géométrique, photométrique, et radiométrique de l'objet sur les différentes perspectives.
3. Des défis spécifiques peuvent être demandés : faire tourner l'objet, le présenter sous un éclairage commandé, ou le placer à côté d'un élément de référence.
4. La cohérence des reflets, des ombres, et des caractéristiques physiques de l'objet entre les différentes perspectives confirme son authenticité.
5. Le rapport généré certifie l'état réel de l'objet à l'instant T.

5.6 Sixième mode - Inspection de salle sécurisée

Un responsable de sécurité souhaite vérifier l'intégrité d'une salle de coffres ou d'une réserve de musée suite à une alerte ou de manière routinière.

1. Un agent sur site utilise deux dispositifs pour filmer l'espace.
2. Le serveur commande des séquences de vérification spécifiques : panoramique synchronisé, focus sur les points d'accès, vérification de la présence des éléments inventoriés.
3. La boucle optique entre les dispositifs confirme leur présence physique réelle dans l'espace.
4. Les captures multi-angles permettent de vérifier la cohérence spatiale de l'environnement, détectant toute tentative de substitution par des images préenregistrées.
5. L'historique des vérifications crée une chaîne de preuves consultable.

5.7 Techniques et éléments considérés annexes, et potentiellement nouveaux et/ou spécifiques

Les éléments suivants sont présentés à titre indicatif et non limitatif.
Ils illustrent des approches et concepts que l'inventeur considère comme annexes au protocole principal, potentiellement nouveaux et/ou spécifiques à la présente invention, ainsi que le potentiel offert par la corrélation multi-capteurs et multi-dispositifs dans le cadre de la vérification d'authenticité, sans pour autant restreindre la portée des revendications aux seuls éléments ici décrits.

A) MONO-DISPOSITIF AVEC SURFACE RÉFLÉCHISSANTE - DOUBLE PERSPECTIVE SIMULTANÉE :

Configuration où l'utilisateur exploite une surface réfléchissante pour obtenir deux perspectives simultanées avec un seul dispositif équipé de caméras avant et arrière :

Variante 1 - Face à la surface réfléchissante :
- L'utilisateur se place face à une surface réfléchissante
- Il pointe la caméra frontale et l'écran vers la surface réfléchissante
- La caméra arrière, orientée vers lui, filme son visage directement
- La caméra frontale filme son visage à travers le reflet
- Résultat : deux perspectives du même sujet capturées simultanément
- L'utilisateur déplace le dispositif selon les instructions, générant des variations géométriques analysables

Variante 2 - Surface réfléchissante derrière l'utilisateur :
- L'utilisateur tient le dispositif en mode selfie (écran face à lui)
- Une surface réfléchissante est positionnée derrière lui
- La caméra frontale capture le visage de l'utilisateur
- La caméra arrière capture le reflet de la scène (incluant potentiellement le dos de l'utilisateur, l'environnement, et/ou le reflet du dispositif)
- Multiples configurations géométriques possibles selon le positionnement

Éléments de vérification exploitables durant ces configurations :
- Déclenchement du flash (effets lumineux cohérents sur les deux captures)
- Affichage de séquences visuelles sur l'écran (visibles dans le reflet)
- Contrôle de l'éclairage ambiant : l'utilisateur peut éteindre la lumière de la pièce, permettant de contrôler la luminosité et colorimétrie via l'écran (séquences de couleurs, variations d'intensité) et/ou le flash (clignotements commandés)
- La cohérence des effets lumineux entre les deux perspectives (directe et reflétée) constitue un facteur de vérification supplémentaire

B) CHAÎNE DE CAPTURE / PONT DE PERSPECTIVE :

Technique où un dispositif capture une scène via une caméra, puis rediffuse ce flux sur son écran, permettant à une autre source de capture (sur un autre dispositif ou sur le même dispositif via surface réfléchissante) d'observer ce flux rediffusé tout en capturant simultanément la scène sous un angle différent.

Principe fondamental :
- Un dispositif capture un flux via une ou plusieurs de ses caméras
- Ce flux peut être affiché localement et/ou transmis au serveur
- Le serveur peut renvoyer le flux (altéré ou non) au même dispositif ou à un autre dispositif pour affichage
- L'affichage résultant peut être observé par d'autres sources de capture

EXEMPLES DE CONFIGURATIONS (indicatifs et non limitatifs) :

Exemple 1 - Flux back cam via serveur :
- Le téléphone capture avec sa caméra arrière (ex: filme le visage de l'utilisateur)
- Le flux est envoyé au serveur
- Le serveur renvoie le flux au même téléphone
- Le téléphone affiche ce flux sur son écran (face avant)
- Le flux affiché est donc ce que la caméra arrière a capturé, après transit serveur

Exemple 2 - Flux front cam local immédiat :
- Le téléphone capture avec sa caméra frontale
- Le flux est affiché immédiatement sur son propre écran, sans passer par le serveur
- Des altérations peuvent être appliquées localement (formes, couleurs, éléments visuels), commandées ou non par le serveur

Exemple 3 - Flux front cam via serveur avec altération :
- Le téléphone capture avec sa caméra frontale
- Le flux est envoyé au serveur
- Le serveur altère le flux (injection d'éléments de vérification, stéganographie, modifications visuelles) ou le renvoie tel quel
- Le téléphone reçoit et affiche le flux sur son écran

Exemple 4 - Split screen double caméra sur même dispositif :
- Le serveur commande au téléphone d'afficher en écran partagé :
  * Une moitié : flux de la caméra arrière
  * Autre moitié : flux de la caméra frontale
- Chaque flux peut transiter ou non par le serveur avant affichage
- Les deux flux sont affichés côte à côte sur le même écran

Exemple 5 - Split screen avec caméra distante :
- Le téléphone affiche en écran partagé :
  * Une moitié : flux de sa propre caméra frontale
  * Autre moitié : flux de la caméra d'un second dispositif, streamé à distance
- Le flux du second dispositif peut transiter par le serveur ou être transmis en peer-to-peer
- Permet d'observer simultanément deux perspectives sur le même écran

Note : Toutes les combinaisons de ces configurations, qu'elles soient décrites ou non décrites ci-dessus, sont considérées comme des configurations de test potentielles pour la présente invention. Cela inclut, sans s'y limiter : toute combinaison de caméras (front, back, multiples), tout routage de flux (local, serveur, peer-to-peer), toute disposition d'affichage (plein écran, split screen, picture-in-picture), et toute altération (locale ou serveur).

Cela inclut également tout mode d'affichage de données, y compris les représentations visuelles de données non-visuelles (incluant, sans s'y limiter : visualisation de flux audio, données radiométriques, données télémétriques, données inertielles, ou toute autre donnée capteur), ainsi que tout effet visuel dont les caractéristiques (couleur, forme, animation, intensité, ou autre) sont dérivées directement ou indirectement d'un flux de données, que celui-ci soit commandé par le serveur (arbitrairement ou pas, aléatoirement ou pas) ou basé sur des données collectées localement par le dispositif.

Application du principe :
- Une seconde source de capture observe cet écran (flux "pass-through") tout en voyant également la scène/l'utilisateur sous un autre angle

Configuration multi-dispositifs :
- Dispositif A : caméra arrière filme l'utilisateur, écran affiche le flux
- Dispositif B : observe l'écran de A (voit le flux pass-through) ET observe l'utilisateur directement sous un angle différent
- Le serveur reçoit : le flux original de A + le flux de B contenant à la fois le retour d'écran et une perspective différente de l'utilisateur
- Vérification de cohérence entre le flux original et sa rediffusion capturée, plus corrélation avec la perspective alternative

Configuration mono-dispositif avec surface réfléchissante :
- Caméra arrière filme l'utilisateur (son visage)
- Flux rediffusé sur l'écran après passage par le serveur
- Caméra frontale, orientée vers une surface réfléchissante, capture :
  * Le reflet de l'écran (montrant le flux pass-through de la caméra arrière)
  * Le reflet du visage de l'utilisateur sous un angle différent
- Résultat : deux perspectives du même sujet + vérification du transit serveur

Avantages de cette technique :
- Prouve que le flux transite effectivement par le serveur (pas de simulation locale possible sans accès au flux rediffusé)
- Permet l'injection d'éléments de vérification dans le flux rediffusé (stéganographie, marqueurs visuels, modifications subtiles)
- Corrélation multi-angle vérifiable sur une même frame temporelle
- Défis de positionnement exploitables (demander à l'utilisateur de bouger, vérifier cohérence des deux perspectives + flux pass-through)

Contrôle opaque par le serveur :
Le contrôle du flux par le serveur présente un avantage supplémentaire : le traitement appliqué est opaque pour l'attaquant. Ce dernier ne peut pas prédire quelles modifications, injections, ou éléments de vérification le serveur va appliquer au flux avant rediffusion. Même en cas de compromission du dispositif local, le serveur conserve le contrôle de ce qui est affiché, rendant toute tentative de simulation locale inefficace.

C) RÉCURSION VISUELLE (BOUCLE DE RÉTROACTION OPTIQUE) :

Technique où une source de capture observe, directement ou indirectement, sa propre sortie visuelle (son propre écran), créant un effet de mise en

abyme (récursion infinie) dont les caractéristiques sont analysables.

Principe fondamental :
- L'écran d'un dispositif affiche un flux
- Une caméra (du même dispositif ou d'un autre) capture cet écran
- Le flux capturé est lui-même affiché, créant une boucle récursive
- L'effet visuel résultant (mise en abyme / "effet tunnel") possède des propriétés géométriques et temporelles spécifiques à la configuration physique réelle

Configuration multi-dispositifs :
- Dispositif A et B positionnés face à face
- Écran de A visible par caméra de B, et vice versa
- Chaque dispositif voit l'écran de l'autre, créant une récursion croisée
- L'effet de mise en abyme apparaît dans les deux flux

Configuration mono-dispositif avec surface réfléchissante :
- Dispositif positionné face à une surface réfléchissante
- L'écran se voit lui-même via le reflet
- La caméra capture ce reflet, incluant l'image de l'écran
- Boucle de rétroaction créée sans second dispositif

Propriétés vérifiables :
- Géométrie de la récursion (angles, distorsions, proportions des "niveaux")
- Délais temporels entre les niveaux de récursion (latence visible)
- Cohérence des éléments affichés à travers les niveaux
- Réponse aux stimuli commandés (changement de couleur, flash) propagée dans la récursion avec délais caractéristiques

Difficulté de simulation :
- Simuler une récursion visuelle convaincante requiert un rendu récursif en temps réel, computationnellement prohibitif
- Chaque niveau de récursion multiplie la complexité du rendu
- Les délais temporels authentiques sont difficiles à reproduire
- La géométrie dépend de la configuration physique réelle (angles, distances)

D) RECONSTRUCTION DYNAMIQUE ET COHÉRENCE :

Technique exploitant les images capturées durant les mouvements de l'utilisateur pour reconstruire partiellement la scène et vérifier sa cohérence géométrique.
Compatible avec les configurations mono-dispositif (multi-caméras) :
même sur un seul dispositif, l'utilisation de plusieurs caméras apporte une diversité angulaire qui augmente la difficulté de falsification sans nécessiter de second appareil.
Également compatible avec les configurations multi-dispositifs.

Principe fondamental :
- Basé sur les images capturées pendant que l'utilisateur tourne, se déplace, bouge, ou exécute les défis physiques, on identifie des éléments de référence dans la scène
- On compare ces éléments lorsqu'ils réapparaissent dans le champ de capture (cohérence géométrique, proportions, positions relatives)

- Le système infère également la distance et position spatiale des éléments de la scène dans l'espace 3D, permettant de reconstruire partiellement ou totalement la géométrie de l'environnement
- Un simulateur devrait maintenir une cohérence 3D complète de l'environnement tout au long de la séquence - extrêmement difficile en temps réel

Intégration des techniques de détection existantes :
- Le système peut également exploiter, en complément de l'analyse de cohérence multi-perspectives, les techniques de détection existantes (incluant, sans s'y limiter : analyse d'artefacts visuels, analyse de texture cutanée, détection de micro-expressions, analyse fréquentielle, détection de compression/recompression, analyse des reflets cornéens et spéculaires), ces techniques bénéficiant d'une fiabilité accrue lorsqu'appliquées de manière corrélée sur plusieurs angles de capture
- Les techniques basées sur l'analyse des reflets peuvent être combinées avec l'émission de signaux visuels commandés (flash, séquences lumineuses sur écran, variations de luminosité, tel que décrit dans les autres sections), permettant de vérifier la cohérence des reflets observés depuis plusieurs perspectives par rapport aux stimuli émis

Variation de vitesse comme facteur de vérification :
- Le système peut demander différentes vitesses de mouvement (rotation lente, puis rapide, puis arrêt brusque)
- Les artefacts de capture (motion blur, rolling shutter, compression) varient naturellement avec la vitesse
- Un simulateur devrait reproduire ces artefacts de manière cohérente avec la vitesse demandée et les caractéristiques du capteur

Exploitation des imperfections et comportements caméra :
- Rolling shutter : distorsion caractéristique lors de mouvements rapides, spécifique au capteur physique
- Motion blur naturel : flou de mouvement cohérent avec la vitesse réelle
- Artefacts de compression vidéo : comportement prévisible mais difficile à simuler correctement
- Latence de l'autofocus : temps de mise au point caractéristique
- Variations d'exposition automatique : adaptation à la luminosité ambiante
- Ces comportements sont intrinsèques au matériel et difficiles à reproduire fidèlement dans une simulation

Analyse temps réel et/ou post-processing :
- L'identification des éléments de référence peut être effectuée en temps réel (feedback immédiat) ou a posteriori (analyse plus approfondie)
- Le post-processing permet des algorithmes plus lourds : reconstruction 3D complète, vérification de cohérence géométrique exhaustive

E) CORRÉLATION INERTIELLE, POSITIONNELLE ET VISUELLE :

Technique exploitant la corrélation entre les données des capteurs inertiels et positionnels (incluant, sans s'y limiter : accéléromètre, gyroscope, orientation, GPS, GNSS, capteurs ToF 3D, lidar, ou tout capteur futur capable de fournir des données de position, déplacement ou inertie) et l'inférence de mouvement dérivée des images capturées. Compatible avec les configurations

mono-dispositif et multi-dispositifs.

Principe fondamental :
- Le dispositif enregistre ses mouvements et/ou sa position via les capteurs inertiels et positionnels (IMU, GPS, GNSS, ToF, lidar, ou équivalent)
- Le système infère le mouvement/déplacement du dispositif à partir des images capturées, et/ou détermine ce qui est attendu visuellement à partir des données inertielles/positionnelles, par tout moyen technique approprié (incluant, sans s'y limiter : algorithmes de vision par ordinateur, apprentissage automatique, intelligence artificielle, simulation numérique, ou toute méthode computationnelle présente ou future)
- Ces sources de données (inertielles, positionnelles et visuelles) doivent être cohérentes entre elles
- Le système peut également inférer la distance et position spatiale des éléments de la scène (objets, surfaces, sujet) à partir des images capturées, et vérifier la cohérence de cette géométrie avec les données des capteurs de profondeur/distance si disponibles, ou par recoupement multi-perspectives
- Toute incohérence entre le mouvement/position mesuré par les capteurs, le mouvement apparent dans les images, et/ou la géométrie spatiale inférée de la scène, constitue un indicateur de falsification

Difficulté pour un attaquant :
- Un simulateur devrait non seulement générer des images convaincantes, mais aussi simuler les données inertielles et positionnelles de manière parfaitement cohérente avec les mouvements visuels rendus
- Cette simulation multi-sources synchronisée (visuel + inertiel + positionnel) est extrêmement difficile à réaliser de manière convaincante
- Les micro-variations, vibrations, et mouvements subtils captés par les capteurs sont particulièrement difficiles à reproduire en cohérence avec le visuel et les données positionnelles

Avantage asymétrique temporel :
- L'attaquant doit simuler en TEMPS RÉEL (contrainte forte de latence)
- Le serveur/vérificateur peut analyser les données A POSTERIORI sans contrainte de temps réel
- Pour les opérations à enjeux élevés, la validation peut être asynchrone
- Le post-processing permet des analyses plus profondes : reconstruction 3D, vérification de cohérence géométrique complète, corrélation fine des micro-mouvements
- Cette asymétrie temporelle constitue un avantage structurel majeur du système

Sources d'inférence de mouvement visuel (incluant, sans s'y limiter) :
- Changements de perspective géométrique entre frames
- Parallaxe (déplacement différentiel objets proches/lointains)
- Flux optique (optical flow)
- Transformations affines/projectives entre images successives
- Variations de la zone visible de la scène
- Décalages temporels inter-capteurs (en configuration multi-caméras)

F) TECHNIQUES ACOUSTIQUES AVANCÉES ET CORRÉLATION MULTI-MICROPHONES :

L'utilisation corrélée de plusieurs microphones répartis sur des dispositifs

distincts, dans le cadre d'un processus de vérification d'authenticité ou de détection de falsification, constitue une composante du présent protocole. Les techniques suivantes sont exploitables individuellement ou en combinaison.

Effet Doppler comme facteur de vérification :
- Un dispositif émet un signal sonore continu (ton pur ou séquence connue) pendant que l'utilisateur effectue des mouvements (rotation, déplacement, gesticulation)
- Un dispositif fixe (ou tenu différemment) capte le décalage de fréquence Doppler proportionnel à la vitesse relative de la source
- Le dispositif émetteur, dans le même référentiel que la source, ne perçoit PAS ce décalage Doppler sur son propre microphone
- Cette asymétrie entre ce que capte le dispositif mobile vs le dispositif fixe est vérifiable et difficile à simuler
- La corrélation avec les données inertielles et visuelles de mouvement renforce la vérification

TDOA (Time Difference of Arrival) et localisation spatiale :
- Le son émis par l'utilisateur (voix) ou par un dispositif arrive à des instants différents sur chaque microphone selon les distances
- Ces différences temporelles permettent de trianguler la position de la source sonore
- La position inférée doit être cohérente avec la position visuelle observée depuis les différentes caméras
- Toute incohérence entre position acoustique et position visuelle constitue un indicateur de falsification

Ombre acoustique et obstruction :
- Lorsque l'utilisateur se déplace, son corps peut bloquer ou atténuer certains chemins de propagation sonore entre dispositifs
- Ces patterns d'obstruction sont prévisibles géométriquement et vérifiables
- La corrélation entre l'ombre acoustique observée et la position visuelle de l'utilisateur constitue un facteur de vérification

Signature acoustique environnementale (Room Impulse Response) :
- Chaque espace physique possède une empreinte acoustique unique (réverbération, échos, absorption fréquentielle)
- Cette empreinte doit être cohérente sur tous les microphones présents dans le même espace
- Une simulation devrait reproduire cette empreinte de manière cohérente sur plusieurs flux audio simultanés

Corrélation de phase et cohérence spectrale :
- Les signaux captés par différents microphones présentent des décalages de phase prévisibles selon la géométrie
- L'analyse de cohérence spectrale entre microphones permet de vérifier la co-localisation des dispositifs

Objet externe comme source sonore :
- L'objet de vérification dédié (décrit dans les autres sections) peut également servir de source d'émission sonore commandée
- Tout objet introduit dans la scène peut être utilisé comme source de son

(manipulation, choc, vibration) dont les caractéristiques acoustiques sont analysables depuis plusieurs microphones
- La cohérence entre le son capturé et le geste visible de l'utilisateur (lip-sync, bruits d'interaction, manipulation d'objets) renforce la vérification

Analyse vocale multi-perspectives :
- La voix de l'utilisateur, captée depuis plusieurs microphones à distances différentes, présente des caractéristiques d'atténuation et de réverbération prévisibles
- La distance inférée acoustiquement doit correspondre à la distance visuelle estimée depuis les caméras
- Les variations d'intensité lors des mouvements de l'utilisateur doivent être cohérentes avec les mouvements observés visuellement

G) DÉTECTION D'ALTÉRATION PARTIELLE DU FLUX (DEEPFAKE LOCALISÉ) :

Problème ciblé :
Un scénario d'attaque sophistiqué consiste à utiliser un flux de caméra majoritairement authentique, mais où seule une portion de l'image est altérée ou générée artificiellement (typiquement : le visage de l'utilisateur). Dans ce cas, l'environnement, l'éclairage, les objets et le contexte général sont réels, rendant la détection plus difficile car la majorité du flux est authentique.

Contre-mesures intrinsèques au protocole (à titre illustratif - ces protections découlent naturellement des éléments techniques généralement décrits dans le présent document) :

1) Rétroaction visuelle (récursion / mise en abyme) :
La boucle de rétroaction optique rend cette attaque particulièrement difficile en temps réel : l'attaquant doit altérer le visage non seulement dans le flux original, mais également dans TOUTES les rediffusions et reflets de ce flux. Chaque niveau de récursion multiplie la complexité de l'altération cohérente.

2) Défis de dissimulation et d'exposition multi-angles :
- Défis demandant de cacher momentanément le visage (main devant le visage, rotation de tête, passage d'un objet) : les transitions et cas limites révèlent les artefacts du deepfake
- Défis exposant le visage simultanément sous plusieurs angles (via plusieurs dispositifs ou via surface réfléchissante) : l'altération doit être géométriquement cohérente sur TOUTES les perspectives en même temps
- Variante avancée : demander à l'utilisateur de passer un appareil avec écran devant son visage, face à une autre caméra. Sur cet écran, afficher des patterns visuels conçus pour confondre les modèles d'altération :
  * Fragments de visages (potentiellement celui de l'utilisateur, avec légères déformations)
  * Patterns adversariaux anti-IA (à définir/développer, pouvant ou non relever de la présente invention)

* Formes et textures conçues pour perturber la détection/génération faciale automatisée

Dans ce scénario, tout modèle ou technologie d'altération tentant de créer un faux flux vidéo pour remplacer/altérer/simuler ce qui est capturé par la caméra faisant face à l'utilisateur serait confronté à ces éléments visuels perturbateurs, rendant la génération cohérente d'un visage de remplacement significativement plus difficile.

3) Chaîne de capture / Pont de perspective comme vérification d'intégrité :

Cette technique devient particulièrement pertinente ici. Le dispositif capturant (ex: téléphone) est lui-même visible depuis le second dispositif (ou via surface réfléchissante). Cela permet de confirmer :

- L'intégrité physique relative de l'appareil (un iPhone qui s'annonce comme tel, sans matériel externe branché dessus, sans câbles suspects)
- La réalité du modèle d'appareil utilisé
- L'absence de dispositif d'interception ou de modification externe visible

4) Double altération requise avec transit serveur :

Pour illustrer : dans un scénario de chaîne de capture où la caméra arrière est pointée vers le visage de l'utilisateur, et où l'écran avant du même appareil rediffuse ce flux après passage par le serveur (visible par un second appareil).

Lorsque le flux transite ainsi par le serveur avant rediffusion sur le même appareil, l'attaquant doit compromettre :

- La capture initiale (altérer le visage dans le flux initialement capturé)
- ET le flux retour du serveur (altérer à nouveau le visage dans le flux rediffusé, sachant que le serveur peut avoir injecté des modifications)

Cette double altération doit se faire en temps réel, sur un appareil dont la présence physique est confirmée visuellement, et qui n'a pas lui-même la puissance de calcul nécessaire pour effectuer cette simulation et double altération en direct.

De plus, le serveur peut renvoyer un flux partiellement altéré de manière imprévisible, rendant le remplacement du visage avant affichage impossible à anticiper.

EXEMPLE ILLUSTRATIF - ANALYSE DE LA COMPLEXITÉ D'ATTAQUE :

Pour illustrer la profondeur de protection, considérons le scénario d'attaque suivant et ses implications :

Configuration de l'attaque (hypothétique) :
Un attaquant tente d'utiliser un téléphone réel visible dans la scène, mais dont le flux vidéo est intercepté et altéré par un équipement externe (rig de simulation/altération) avant d'être renvoyé vers les destinations.

Flux de données nécessaires à l'attaquant (minimum) :
- Stream 1 : Caméra du téléphone → Rig externe de simulation/altération
- Stream 2 : Rig → Téléphone (flux altéré à afficher sur l'écran)
- Stream 3 : Téléphone → Serveur (flux altéré envoyé au serveur)

- Stream 4 : Serveur → Téléphone (flux retour, potentiellement ré-altéré)

Dans certaines configurations, ce sont 4 streams vidéo haute qualité, en temps réel, avec latence minimale. Même si certains streams peuvent être optimisés ou combinés (ex: si la simulation est bien faite, le retour serveur pourrait être rerouté, voire le téléphone et/ou notre application pourrait être entièrement virtualisé dans un rig externe, le téléphone physique visible dans la scène ne servant plus que d'interface ou de coquille vide affichant les sorties du rig), un MINIMUM de 2 streams sans fil haute qualité reste nécessaire.

Contraintes physiques révélatrices :
- Les défis techniques imposent des mouvements libres et amples de l'appareil
- Un câble physique reliant l'appareil à un rig externe :
  * Serait visible par le dispositif de vérification (sauf altération d'image)
  * Gênerait les mouvements amples demandés par les défis
  * Les tests doivent être conçus en prenant en compte cette contrainte (mouvements circulaires, retournements complets, etc.)
- Une connexion sans fil implique des émissions radio détectables

Détection par analyse radiométrique :
Si d'autres dispositifs contrôlés par le vérificateur ont accès à l'analyse radiométrique de l'environnement (scan WiFi, Bluetooth, spectres radio), ils peuvent détecter :
- Des flux de données suspects en cours, au-delà des communications attendues
- Des volumes de trafic WiFi/radio anormaux pour la situation
- Des patterns de communication non expliqués par la configuration déclarée

Variante avancée - corrélation contenu/bande passante :
Le serveur peut volontairement introduire des variations de complexité visuelle dans le flux rediffusé (ex: flash blanc, écran uniforme, puis scène complexe). Une image uniforme compresse significativement mieux qu'une image complexe (principe d'entropie exploité par les codecs vidéo). Le profil de bande passante attendu "sur le canal sans fil" (over the air) devient donc prédictible et corrélé au contenu affiché.

Cette évaluation peut également être effectuée de manière routinière, sans introduire de complexité ou simplicité artificielle, en comparant simplement le profil de bande passante observé dans l'environnement radio avec celui attendu pour le flux connu. Certes, un attaquant pourrait utiliser un stream à débit fixe ou aléatoire pour contourner cette mesure - il ne s'agit que d'une piste parmi d'autres, non d'une protection absolue.

Note : un environnement radio suffisamment propre peut être posé comme condition préalable au test, au même titre qu'une latence suffisamment faible ou des écrans/caméras de qualité décente.

Si l'attaquant utilise des streams parallèles, la variation de débit de ses flux ne correspondrait pas au profil attendu. La cohérence de ces flux, l'effacement des harmoniques vis-à-vis de l'environnement radiométrique qu'il nous transmet (lui-même potentiellement falsifié), serait significativement plus difficile à simuler pour l'attaquant qu'à vérifier de notre côté.

Même si ces flux sont chiffrés, le VOLUME et la PRÉSENCE des communications sont détectables. L'attaquant devrait donc également :
- Masquer ses propres signaux radio des scans environnementaux
- Laisser visible uniquement les signaux "normaux" attendus
- Cacher les harmoniques et signatures radio de son équipement
- Le tout en temps réel, sans latence perceptible

Note sur l'expérience utilisateur :
Du point de vue de l'utilisateur, ce test reste relativement simple sur le plan physique (tenir un appareil, effectuer quelques mouvements). Les contraintes en termes de durée et d'attention sont largement justifiables pour des opérations à enjeux élevés : un utilisateur acceptera volontiers de consacrer 30 secondes, voire 3 minutes, à un tel processus de vérification si ses économies d'une vie ou une transaction critique sont en jeu.

Conclusion de l'exemple :
La combinaison de la vérification visuelle de l'intégrité physique de l'appareil, du transit serveur avec double altération requise, des contraintes de mouvement libre, et de l'analyse radiométrique potentielle, rend ce type d'attaque par altération partielle d'une complexité prohibitive, nécessitant un niveau de sophistication et de ressources disproportionné par rapport à la vérification.

H) OBJETS SECONDAIRES DE VÉRIFICATION :

Le protocole peut intégrer des objets physiques comme facteurs de vérification additionnels. Ces objets constituent un facteur d'authentification supplémentaire (quelque chose que l'utilisateur POSSÈDE), complémentaire aux facteurs biométriques et comportementaux déjà décrits.

H.1) Objets du quotidien (rappel - ancres d'entropie) :

Tel que décrit précédemment dans le présent document, des objets ordinaires (bouteille d'eau, tissu, objets déformables, liquides, ou tout autre objet présentant un comportement physique observable) peuvent servir d'ancres d'entropie dont le comportement chaotique est vérifié sous plusieurs angles.

Cette catégorie inclut également des objets génériques disponibles dans le commerce, non conçus pour l'authentification mais présentant des comportements physiques complexes et difficiles à simuler, tels que (non limitatif) :
- Sabliers avec dynamique de particules
- Boules à neige ou globes avec particules en suspension
- Objets lumineux avec comportements variables
- Jouets ou gadgets avec mouvements chaotiques
- Tout objet présentant un comportement physique observable et imprévisible

Cette catégorie est mentionnée ici pour mémoire et complétude.

H.2) Objets associés au compte - Dédiés ou non à l'authentification :

Le protocole peut intégrer tout objet physique, dédié ou non à l'authentification, comme facteur de vérification complémentaire. L'objet est associé au compte utilisateur et sa possession constitue une preuve d'identité, utilisable seule ou en combinaison avec d'autres facteurs.

A) OBJETS DÉDIÉS À L'AUTHENTIFICATION :

Accessoires physiques conçus pour l'authentification, fournis à l'utilisateur ou acquis séparément. Formes possibles (non limitatif) : tag, porte-clés, carte, bracelet, bijou, badge, ou tout autre objet portable.

Tag passif (technologie existante, intégrée au protocole) :
- Puce RFID, NFC, ou équivalent, sans alimentation propre
- L'utilisateur présente ou scanne l'objet pendant la vérification
- Vérifie la possession physique d'un objet associé au compte
- Lecture par proximité (near field) ou par capture visuelle (QR code, marquage)

Tag actif avec génération de code dynamique (technologie existante, intégrée) :
- Puce avec électronique embarquée et source d'alimentation
- Génère une valeur temporelle (TOTP - Time-based One-Time Password, ou équivalent) basée sur une clé secrète partagée avec l'entité de vérification
- L'objet affiche ou transmet un code qui change périodiquement
- Similaire aux tokens d'authentification existants (RSA SecurID ou équivalents)

B) OBJETS NON DÉDIÉS - OBJETS DU QUOTIDIEN ASSOCIÉS AU COMPTE :

L'utilisateur peut associer à son compte des objets pré-existants, non conçus pour l'authentification mais contenant des données fixes et lisibles. Ces objets servent de facteur de vérification complémentaire.

Exemples d'objets associables (non limitatif) :
- Carte bancaire : numéro (PAN) lisible par NFC ou par capture visuelle (OCR)
- Badge d'immeuble ou d'entreprise : identifiant unique (UID) lisible par NFC/RFID
- Carte de transport : Navigo, Oyster, ou équivalent, avec UID unique
- Clé de voiture connectée : identifiant Bluetooth ou NFC
- Carte de fidélité avec puce ou code-barres
- Passeport ou carte d'identité avec puce NFC (données publiques)
- Tout autre objet contenant un identifiant fixe lisible électroniquement ou visuellement

Données exploitables (non limitatif) :
- Identifiant unique (UID) de puce RFID/NFC
- Numéro de série, numéro de carte, ou autre donnée statique
- Code-barres, QR code, ou marquage visuel
- Caractéristiques physiques distinctives (forme, couleur, usure)
- Toute donnée fixe permettant d'identifier l'objet de manière unique

C) COMBINAISONS ET USAGES :

- Tag dédié + objet non dédié en combinaison
- Caractéristiques physiques vérifiables visuellement (forme, couleur, marquages, hologrammes) capturées par les sources de capture multi-angles

- Toute combinaison des éléments ci-dessus

D) OBJETS DE CONFIANCE POUR RÉCUPÉRATION DE COMPTE :

L'utilisateur peut désigner un ou plusieurs objets (dédiés ou non) comme "objets de confiance" pour la récupération de compte. En cas de perte d'accès (téléphone perdu, oubli de mot de passe, etc.), la possession de l'objet de confiance, combinée à une vérification biométrique réalisée depuis n'importe quel appareil (y compris un appareil ne lui appartenant pas), permet de rétablir l'accès au compte.

Cas d'usage :
- L'utilisateur confie un objet de confiance à un proche (ami, famille)
- L'utilisateur dépose un objet dans un lieu sécurisé (coffre, casier)
- En cas de besoin, l'utilisateur récupère l'objet et prouve son identité depuis un appareil tiers (téléphone d'un ami, borne publique, etc.) par : objet de confiance + vérification biométrique live

Cette approche offre une alternative aux méthodes de récupération traditionnelles (email, SMS, questions secrètes) avec une sécurité renforcée.

Variantes et évolutions futures :

- Objet de confiance implanté : l'objet peut être un implant sous-cutané, dentaire, ou autre, éliminant le risque de perte ou d'oubli. L'utilisateur porte en permanence son facteur de récupération.

- Récupération sans objet physique (évolution technologique) : si les moyens technologiques le permettent, la vérification biométrique et physiologique seule (sans objet de confiance) pourrait suffire à garantir l'identité de l'utilisateur en scénario de récupération. Cette configuration est couverte par le présent protocole, où les marqueurs biométriques et physiologiques (empreinte faciale, vocale, comportementale, rétinienne, ou tout autre marqueur identifiant de manière unique l'individu) constituent le facteur de récupération, sans nécessiter d'objet physique externe.

Le protocole couvre ainsi un spectre allant de :
- Objet externe + biométrie (configuration actuelle)
- Objet implanté + biométrie (configuration intermédiaire)
- Biométrie seule (configuration future, si technologiquement suffisante)

Note : Les technologies de tags passifs et de génération TOTP constituent un état de l'art connu. Leur intégration dans le présent protocole de vérification multi-dispositifs est décrite à titre d'option complémentaire, sans revendication d'une possibilité de nouveauté sur ces technologies en elles-mêmes.

H.3) Objets physiques intelligents à comportement réactif unique :

REVENDICATIONS DE CONCEPTS - TIERS INDÉPENDANTS ET COMBINABLES :

La présente invention couvre les concepts suivants, revendiqués séparément et en toute combinaison. Chaque tier constitue une invention en soi,

applicable dans le contexte du présent protocole unifié ou indépendamment.
L'objet peut être connecté (Bluetooth, NFC, WiFi, filaire, ou autre) ou
non connecté. L'objet peut être activable/désactivable par l'utilisateur
ou fonctionner de manière permanente.

TIER A - COMPORTEMENT RÉACTIF INTERACTIF (indépendamment de toute clé) :

Objet physique caractérisé par un comportement réactif à des stimuli
externes, où la réaction constitue un élément de vérification observable.
L'interactivité en soi (et non un simple passage ou relais de signal)
constitue le cœur de ce concept.

Stimuli d'entrée possibles (non limitatif) :
- Optiques : lumière ambiante, flash, patterns lumineux, laser
- Acoustiques : son, ultrasons, patterns sonores
- Électromagnétiques : signal radio, NFC, Bluetooth, WiFi
- Data : commandes numériques via connexion
- Physiques : température, pression, mouvement, orientation
- Tout autre stimulus mesurable par un système ou un capteur

Réactions de sortie possibles (non limitatif) :
- Lumineuse : LED, écran, changement de couleur
- Sonore : bip, mélodie, pattern acoustique
- Vibratoire : moteur haptique
- Mécanique : mouvement, rotation, déploiement
- Électromagnétique : émission radio, NFC
- Thermique : changement de température
- Toute autre réaction observable ou mesurable

Ce qui distingue ce concept de l'état de l'art (TOTP/SecurID) :
L'objet ne répond pas simplement "quelle heure est-il" mais "qu'ai-je
perçu" - la réaction dépend de stimuli EXTERNES et non uniquement du temps.

MODES DE COMMUNICATION ET D'INTERACTION (non limitatif) :

L'objet peut être communiquant et interactif par TOUT moyen, incluant :

Sans fil :
- Bluetooth (Classic, LE, Mesh), WiFi, Zigbee, Z-Wave, Thread
- NFC, RFID (toute fréquence), UWB (Ultra-Wideband)
- Infrarouge, optique (Li-Fi, communication par lumière visible)
- Cellulaire (LTE-M, NB-IoT, 5G, ou tout réseau mobile)
- LoRa, Sigfox, ou tout protocole LPWAN
- Propriétaire ou standard, existant ou futur

Filaire :
- USB, série, I2C, SPI, ou tout bus de communication
- Ethernet, fibre optique
- Audio jack (communication par signal audio)
- Contact électrique direct
- Tout autre moyen de connexion physique

Passif (sans alimentation propre pour la communication) :
- RFID passif, NFC passif
- Réflexion/modulation de signal externe
- Communication optique par réflexion ou absorption

Unidirectionnel ou bidirectionnel :
- L'objet peut recevoir uniquement (capteur passif)
- L'objet peut émettre uniquement (beacon)
- L'objet peut recevoir ET émettre (communication bidirectionnelle)

Topologie et portée de communication :
- Avec le dispositif principal uniquement (communication locale, directe)
- Avec une entité distante via internet (communication globale)
- Entre objets, formant un réseau maillé (mesh) autonome
- Via des relais ou passerelles intermédiaires
- Toute combinaison de ces modes

Les objets peuvent ainsi former un réseau autonome (LoRa mesh, Bluetooth Mesh, Zigbee mesh, ou tout autre protocole maillé), communiquant entre eux indépendamment du dispositif principal, et/ou relayant des informations vers l'entité de vérification.

L'interactivité couvre toute forme d'échange d'information ou de réaction à un stimulus, quel que soit le médium physique utilisé, quelle que soit la topologie du réseau, et quelle que soit la portée (locale ou globale).

AUTONOMIE, ALIMENTATION ET FONCTIONS ÉTENDUES DES OBJETS :

Niveau d'autonomie (non mutuellement exclusifs) :
- Objet entièrement dépendant du dispositif principal (esclave)
- Objet semi-autonome : peut fonctionner seul mais se synchronise
- Objet entièrement autonome : fonctionne indépendamment, prend des décisions locales, communique de sa propre initiative
- Autonomie variable selon le contexte, l'alimentation, ou la connectivité
- Tout niveau intermédiaire ou combinaison

L'objet peut être conçu comme un nœud intelligent capable de :
- Recevoir, stocker, traiter et retransmettre des messages
- Prendre des décisions locales (logique embarquée, règles, IA)
- Initier des communications (pas seulement répondre)
- Interagir avec d'autres objets sans passer par le dispositif principal
- Former un réseau pair-à-pair (P2P) décentralisé avec d'autres objets
- Relayer des informations entre objets non directement connectés
- Maintenir un état persistant entre les sessions

Fonctions propres (au-delà de l'authentification) :
- Affichage d'informations (heure, notifications, état, messages)
- Interaction utilisateur (boutons, écran tactile, gestes, voix)
- Capteurs environnementaux (température, lumière, humidité, GPS, etc.)
- Actuateurs (vibration, son, lumière, mouvement)
- Stockage de données local (mémoire persistante)
- Calcul et traitement local (microcontrôleur, processeur, FPGA)

- Toute fonction utilitaire, ludique, ou décorative
- Fonctions multiples combinées dans un même objet

L'objet peut avoir une fonction primaire autre que l'authentification (montre, bijou, jouet, outil, décoration, etc.) tout en participant au système de vérification comme fonction secondaire ou intégrée.

Interface utilisateur embarquée (optionnelle) :
- Écran (LCD, OLED, e-ink, LED, ou tout autre affichage)
- Entrées utilisateur : boutons, molette, surface tactile, gestes
- Retour haptique : vibration, feedback tactile
- Audio : haut-parleur, buzzer, synthèse vocale
- Microphone et reconnaissance vocale
- Indicateurs visuels (LEDs, changement de couleur)
- Toute autre forme d'interface homme-machine
- Sans interface visible (objet discret ou invisible)

Sources d'alimentation (non limitatif) :
- Pile unique non rechargeable (pile bouton, AAA, ou autre)
- Batterie rechargeable (lithium, autre chimie, ou future)
- Recharge par induction (Qi, propriétaire, ou autre standard)
- Recharge solaire (cellule photovoltaïque intégrée)
- Recharge par mouvement (cinétique, piézoélectrique)
- Récupération d'énergie ambiante (thermique, RF, vibration)
- Alimentation filaire (USB, contact, ou autre)
- Alimentation passive (énergie fournie par le lecteur NFC/RFID)
- Supercondensateur, pile à combustible, ou toute autre technologie
- Combinaison de plusieurs sources (hybride)
- Sans alimentation propre (objet entièrement passif)
- Toute source d'énergie existante ou future

Durée de vie et maintenance :
- Objet jetable (usage unique ou durée limitée)
- Objet à pile remplaçable par l'utilisateur
- Objet rechargeable par l'utilisateur
- Objet hermétique à durée de vie longue (10+ ans)
- Objet réparable, évolutif, ou mis à jour
- Toute durée de vie et politique de maintenance

INTÉGRATION DANS DOCUMENTS OFFICIELS ET PARTENARIATS INSTITUTIONNELS :

La technologie décrite (comportement réactif unique, identifiant avec secret cryptographique, paramètres variables, ou toute combinaison et/ou déclinaison) peut être intégrée dans des documents officiels existants ou futurs, incluant sans s'y limiter :

Documents d'identité :
- Carte nationale d'identité (CNI, ID card)
- Passeport (biométrique ou non)
- Permis de conduire
- Carte de séjour, titre de séjour

- Carte d'électeur, carte vitale, carte professionnelle
- Tout document officiel délivré par une autorité publique

Autres documents à puce :
- Carte bancaire (débit, crédit, prépayée)
- Badge d'accès professionnel ou institutionnel
- Carte de transport (métro, bus, train, ou équivalent)
- Carte étudiante, carte de bibliothèque
- Carte de fidélité à puce
- Tout support physique contenant une puce électronique

Mode d'intégration :
- Puce NFC/RFID existante enrichie du comportement PICAD
- Puce dédiée ajoutée au document existant
- Nouveau format de document intégrant nativement la technologie
- Mise à jour du firmware de puces existantes (si techniquement possible)
- Application logicielle sur puce à microprocesseur (JavaCard, etc.)
- Toute autre méthode d'intégration matérielle ou logicielle

La puce embarquée dans le document peut ainsi :
- Répondre de manière unique et non reproductible aux stimuli
- Prouver son authenticité via le protocole PICAD
- Participer au réseau d'objets comme nœud de confiance
- Combiner l'identité officielle avec l'authentification PICAD

Modèles de partenariat :
- Intégration gouvernementale : partenariat avec États ou administrations pour l'émission de documents officiels compatibles PICAD
- Intégration bancaire : partenariat avec émetteurs de cartes bancaires
- Intégration institutionnelle : entreprises, universités, organisations
- Intégration tierce : tout partenaire souhaitant ajouter la fonctionnalité à ses propres documents ou dispositifs
- Licence technologique : fourniture de la technologie à des tiers pour intégration dans leurs propres produits
- Standard ouvert ou propriétaire, selon les accords

Cette intégration permet de transformer tout document officiel existant en facteur d'authentification PICAD, sans nécessiter de dispositif supplémentaire dédié, et en bénéficiant de la confiance institutionnelle associée au document d'origine.

AUTHENTIFICATION SÉLECTIVE ET PRÉSERVATION DE LA VIE PRIVÉE :

Le système permet une authentification à divulgation partielle ou nulle : prouver des attributs (âge, appartenance, possession d'objet valide) sans révéler l'identité complète, via des techniques cryptographiques telles que preuves zero-knowledge, signatures aveugles, credentials anonymes, ou toute autre méthode existante ou future permettant la vérification sans divulgation.

RÉVOCATION ET GESTION DES OBJETS COMPROMIS :

Le système permet la révocation d'objets perdus, volés, ou compromis, avec

propagation via l'entité centrale et/ou le réseau mesh (gossip protocol), avec ou sans connexion internet. La révocation peut être permanente, temporaire, ou contextuelle, déclenchée manuellement ou automatiquement.

LOCALISATION ET RECHERCHE D'OBJETS VIA LE RÉSEAU :

Le réseau maillé d'objets peut servir à localiser des objets perdus ou volés de manière collaborative et décentralisée : les objets à proximité relaient l'information vers le propriétaire, avec chiffrement de bout en bout préservant la vie privée. Applications : retrouver un objet, alertes de distance/géofencing, ou audit de localisation.

TIER B - IDENTIFIANT UNIQUE ASSOCIÉ À SECRET CRYPTOGRAPHIQUE :

Objet physique caractérisé par :
- Un identifiant unique lisible (QR code, numéro de série, marquage visuel, puce NFC/RFID, ou tout autre moyen d'identification)
- Un secret cryptographique (clé) associé à cet identifiant, connu de l'entité de fabrication et/ou de vérification
- Le secret n'est PAS stocké de manière lisible sur l'objet (contrairement à l'identifiant)

L'association identifiant-visible ↔ secret-caché permet à une entité tierce de vérifier l'authenticité de l'objet sans que le secret soit exposé.

Ce tier est revendiqué INDÉPENDAMMENT de tout comportement réactif : l'objet peut être entièrement passif (simple support d'identifiant) tout en bénéficiant de l'association avec un secret côté serveur.

TIER C - CODE SOURCE, INSTRUCTIONS DE RÉACTION, ET/OU PARAMÈTRES VARIABLES :

Objet physique dont le comportement est déterminé par un ou plusieurs des éléments suivants, pouvant varier d'un exemplaire à l'autre.

IMPORTANT - Secret ou non-secret : Chacun des éléments ci-dessous (C.1, C.2, C.3) peut être secret OU non-secret (public, connu, peu de variantes). Le concept est couvert indépendamment du caractère secret ou non des éléments. La protection vient de l'unicité par exemplaire et de la connaissance par l'entité de vérification, non du secret en soi.

C.1) Code source / Firmware :
- Le code exécutable (firmware, logiciel embarqué) diffère entre exemplaires
- Peut être statique (fixé à la fabrication) ou dynamique (mis à jour)
- Chaque exemplaire exécute une version ou variante différente du code

C.2) Instructions de réaction / Logique comportementale :
- Les règles définissant comment l'objet réagit aux stimuli
- Peut être encodé dans le code source OU dans des données séparées
- Exemple : "si flash détecté pendant >100ms, émettre séquence X"
- Les instructions peuvent être secrètes ou publiques

C.3) Paramètres de comportement :
- Valeurs numériques, seuils, délais, séquences, tables de correspondance
- Peuvent être stockés séparément du code source
- Peuvent être secrets OU non-secrets (publics, peu de variantes, connus)
- Peuvent être dérivés d'autres données (heure, secret, etc.)

Combinaisons C.1 + C.2 + C.3 :
- Code unique + instructions communes + paramètres communs
- Code commun + instructions uniques + paramètres communs
- Code commun + instructions communes + paramètres uniques
- Toute autre combinaison partielle ou totale

L'entité de fabrication/vérification connaît le code, les instructions, et/ou les paramètres de chaque exemplaire, permettant de prédire et vérifier son comportement.

TIER D - COMBINAISONS :

Les tiers A, B et C peuvent être combinés et intégrés au protocole PICAD de toute manière :

- A seul : objet réactif sans identification unique
- B seul : identifiant avec secret, sans comportement spécial
- C seul : comportement unique, sans identification formelle
- A + B : réaction vérifiable via identifiant connu du serveur
- A + C : réaction unique par exemplaire
- B + C : identifiant + comportement unique
- A + B + C : réaction unique, identifiable, avec secret crypto

La combinaison A + B + C offre le niveau maximal de sécurité :
Réponse = f(stimuli_externes, clé_secrète, code_unique, timing)

Pour un même stimulus, chaque objet produit une réponse différente, et seule l'entité connaissant les paramètres de CET objet peut vérifier.

L'objet peut intégrer un mécanisme d'autodestruction ou de verrouillage en cas de tentative de rétro-ingénierie.

EXEMPLES ILLUSTRATIFS DE MISE EN ŒUVRE :

Les exemples suivants illustrent des configurations possibles sans limiter la portée de la revendication ci-dessus.

Exemple 1 - Objet avec photosenseur et émetteur lumineux :
- L'objet intègre un photosenseur, un émetteur lumineux, et une puce crypto
- L'objet capte la lumière ambiante ou les flashs émis par un dispositif
- L'objet émet une réponse lumineuse calculée selon :
  Réponse = f(lumière_reçue, timing_interne, clé_privée)
- La réponse est captée par une ou plusieurs sources de capture
- L'entité de vérification, connaissant la clé, vérifie la cohérence

Exemple 2 - Objet connecté avec réponse multi-canaux :

- L'objet se connecte à un dispositif via Bluetooth, Zigbee, NFC, connexion filaire, ou tout autre protocole de communication
- L'entité de vérification envoie une valeur X via le canal de données
- Simultanément, le dispositif émet des stimuli physiques (flash, son, etc.)
- L'objet calcule sa réponse selon :
  Réponse = f(valeur_X, stimuli_physiques, timing, clé_privée)
- La multiplicité des canaux d'entrée rend la simulation extrêmement difficile

Exemple 3 - Objet avec capteurs environnementaux :
- L'objet intègre des capteurs additionnels : thermomètre, accéléromètre, hygromètre, ou tout autre capteur de grandeur physique
- La réponse intègre ces mesures environnementales :
  Réponse = f(données_capteurs, signal_reçu, timing, clé_privée)
- Un attaquant devrait reproduire non seulement les signaux mais aussi l'environnement physique exact

PRODUCTION DE MASSE AVEC UNICITÉ :

Chaque exemplaire de l'objet est fabriqué avec :
- Un identifiant unique visible (QR code, numéro de série, marquage, ou autre)
- Une clé cryptographique unique générée lors de la fabrication
- Optionnellement : un code source ou firmware spécifique à cet exemplaire

L'entité productrice maintient une base de données associant chaque identifiant à sa clé et ses paramètres de comportement. Lors de la vérification, l'objet est identifié (par scan, lecture NFC, ou autre), permettant à l'entité de vérification de connaître les paramètres attendus.

MODES D'IDENTIFICATION DE L'OBJET (non limitatif) :
- Capture visuelle (QR code, marquage, forme distinctive)
- Lecture sans contact (NFC, RFID)
- Connexion radio (Bluetooth, Zigbee, WiFi, ou tout protocole)
- Connexion filaire
- Tout autre moyen d'identification électronique ou visuel

DIFFICULTÉ DE SIMULATION :

Pour simuler un tel objet, un attaquant devrait :
- Avoir extrait la clé cryptographique unique de CET objet spécifique
- Avoir rétro-ingénieré le comportement exact (firmware/code source)
- Reproduire en temps réel la réponse correcte aux stimuli imprévisibles
- Sur plusieurs angles de capture simultanés

Cette combinaison de contraintes rend la contrefaçon prohibitivement complexe.

H.4) Détection de continuité de présence pour l'authentification :

REVENDICATION PRINCIPALE - L'APPLICATION EN SOI :

La présente invention revendique l'utilisation de toute méthode de détection de continuité physique, de proximité, ou de présence entre un dispositif et le corps d'un utilisateur, comme facteur d'authentification, de maintien

d'un état d'authentification, ou de vérification d'identité.

Cette revendication couvre l'APPLICATION (l'usage pour l'authentification) indépendamment de la méthode de détection employée, que celle-ci soit connue à ce jour ou développée ultérieurement.

Note : La détection de présence sur montres connectées et téléphones (maintien du déverrouillage tant que porté) constitue un état de l'art existant. L'intégration de ce mécanisme dans le présent protocole est décrite sans revendication de nouveauté sur la détection de présence en elle-même, mais sur : son intégration dans le processus de vérification anti-usurpation, son renforcement par les mécanismes anti-spoofing du protocole PICAD, et ses combinaisons avec les autres éléments décrits (objets réactifs, mesh, etc.).

DISPOSITIFS CONCERNÉS (non limitatif) :

Cette revendication s'applique à tout type de dispositif, dédié ou non à l'authentification, incluant sans s'y limiter :

- Objets dédiés : bracelet, bague, collier, badge, tag, token, pendentif
- Montres connectées (tout fabricant, tout système d'exploitation)
- Téléphones portables : smartphone, téléphone mobile, tablette
- Accessoires audio : écouteurs, casque, oreillette
- Vêtements connectés : textile intelligent, semelle, gant, ceinture
- Implants : sous-cutané, dentaire, ou tout implant corporel
- Lunettes connectées, lentilles connectées, ou équivalent
- Tout autre objet porté sur, dans, ou à proximité immédiate du corps

Le dispositif peut être un produit existant du commerce (montre connectée, téléphone) dont la fonction d'authentification par continuité est activée par logiciel, ou un dispositif conçu spécifiquement pour cette fonction.

MÉTHODES DE DÉTECTION DE PRÉSENCE/CONTINUITÉ (non limitatif) :

Catégorie 1 - Détection physiologique par méthodes optiques/thermiques :
(Les méthodes par électrodes sont couvertes en Catégorie 5)
- PPG (photopléthysmographie) : détection optique du pouls par LED/photodiode
- SpO2 : oxymétrie de pouls (mesure optique)
- Température corporelle : thermomètre de contact ou infrarouge
- Imagerie thermique : caméra infrarouge, distribution de chaleur corporelle
- Pléthysmographie par variation de volume
- Tout autre signal physiologique mesurable par méthode optique ou thermique

Catégorie 2 - Détection mécanique de continuité/fermeture :
- Contact électrique : circuit fermé par contact peau ou fermoir
- Capteur de pression : contact mécanique avec la peau
- Détection d'ouverture de fermoir : interrupteur mécanique ou magnétique
- Capteur de tension/étirement : bracelet qui détecte son propre état
- Circuit conducteur bouclé : fil conducteur dont la rupture est détectée
- Capteur piézoélectrique : détection de pression ou déformation
- Tout autre mécanisme de détection de fermeture ou d'attachement

Catégorie 3 - Détection de proximité/distance :
- Télémétrie optique : mesure de distance par lumière (ToF, LIDAR, IR)
- Télémétrie ultrasonique : mesure de distance par ultrasons
- Télémétrie radio : RSSI Bluetooth, UWB (Ultra-Wideband), WiFi
- Capacitif : détection de présence par champ électrique
- Inductif : détection de présence par champ magnétique
- NFC/RFID : détection de proximité par couplage magnétique
- Radar : détection de présence par ondes radio
- Tout autre méthode de mesure de distance ou proximité

Catégorie 4 - Détection par mouvement/inertie :
- Accéléromètre : détection de mouvement, de marche, de gestes
- Gyroscope : détection d'orientation et de rotation
- Magnétomètre : détection d'orientation par rapport au champ magnétique
- Corrélation de mouvement : le dispositif bouge avec l'utilisateur
- Analyse de la démarche : pattern de mouvement caractéristique
- Tout autre capteur inertiel ou de mouvement

Catégorie 5 - Détection par électrodes de surface et signaux bioélectriques :

Électrodes de contact cutané mesurant les potentiels électriques du corps (gamme typique : µV à mV), incluant sans s'y limiter :

- EMG de surface (électromyographie) : signaux électriques des muscles et neurones moteurs, détection d'intention de mouvement, interface neurale
- ECG/EKG de surface : activité électrique cardiaque via électrodes cutanées
- EEG de surface : ondes cérébrales via électrodes sur le cuir chevelu
- EOG (électro-oculographie) : mouvements oculaires
- EDA/GSR (activité électrodermale) : réponse galvanique de la peau, conductivité cutanée, transpiration
- Bioimpédance : mesure de l'impédance corporelle, composition corporelle, flux sanguin, hydratation
- Signaux nerveux périphériques : activité des nerfs sous la peau
- Potentiels évoqués : réponses électriques à des stimuli

Types d'électrodes couverts :
- Électrodes sèches (sans gel conducteur)
- Électrodes humides/gel
- Électrodes textiles (intégrées dans vêtements)
- Électrodes capacitives (sans contact direct)
- Tout autre type d'électrode ou capteur de potentiel électrique

Champ électromagnétique corporel :
- Variations du champ EM naturel du corps
- Détection passive ou active
- Tout autre signal électromagnétique corporel

Catégorie 6 - Toute autre méthode :
- Toute technologie de détection existante ou future
- Toute combinaison des méthodes ci-dessus
- Tout capteur ou méthode permettant de distinguer la présence ou l'absence du corps de l'utilisateur à proximité du dispositif

TOKEN DE VALIDITÉ ET AUTHENTIFICATION CONTINUE :

Le concept central revendiqué est le suivant :

a) Établissement initial : une authentification forte est réalisée (biométrique, multi-facteur, ou autre) pendant que le dispositif est en contact/proximité avec l'utilisateur

b) Maintien de validité : tant que le dispositif détecte continuellement la présence de l'utilisateur (par une ou plusieurs méthodes ci-dessus), un token ou état de validité est maintenu en mémoire

c) Invalidation automatique : dès que la continuité est rompue (détachement, éloignement, perte de signal physiologique, ouverture de fermoir, ou toute autre interruption de la détection de présence), le token est automatiquement et immédiatement révoqué

d) Ré-authentification requise : après invalidation, une nouvelle authentification complète est nécessaire pour rétablir la validité

e) Niveaux de validité et authentification simplifiée : le token peut maintenir un niveau de confiance qui, tant que la continuité n'est pas rompue, permet une authentification partielle ou simplifiée pour les opérations ultérieures (ex: confirmation par geste simple au lieu de biométrie complète). La rupture de continuité réinitialise ce niveau et exige une authentification complète.

Ce mécanisme s'applique que le dispositif utilise une seule méthode de détection ou plusieurs méthodes combinées (multi-source ou mono-source).

AVANTAGES DE CETTE APPROCHE :

- Sécurité renforcée : le dispositif ne peut pas être prêté, volé, ou transféré sans que le token soit invalidé
- Expérience utilisateur améliorée : pas de ré-authentification répétitive tant que le dispositif reste en présence de l'utilisateur
- Adapté aux contextes à haute exigence : utilisateurs devant prendre des décisions critiques fréquentes (environnements sensibles, transactions à fort enjeu) bénéficient d'une authentification forte sans friction
- Authentification continue : vérification permanente, pas ponctuelle
- Applicable à l'existant : peut être implémenté sur des montres/téléphones existants via mise à jour logicielle

PORTÉE DE LA REVENDICATION :

Cette revendication couvre :
- L'utilisation de toute méthode de détection de continuité/présence/proximité, notamment les méthodes nouvelles ou intégrées au protocole PICAD
- Pour le maintien d'un état d'authentification ou de validité
- Sur tout type de dispositif (dédié ou non, existant ou futur)
- Avec une ou plusieurs méthodes de détection (mono ou multi-source)

- Et notamment dans le contexte du présent protocole (ou indépendamment)

Cette application de la détection de continuité au domaine de l'authentification pour opérations à distance peut constituer une invention en soi.

COMBINABILITÉ DES CONCEPTS H.3 ET H.4 :

Les fonctionnalités décrites en H.3 (comportement réactif unique) et H.4 (détection de continuité de présence) peuvent être combinées dans un même dispositif. Un tel dispositif cumulerait :

- La réactivité unique aux stimuli externes (H.3)
- La détection de présence/continuité par une ou plusieurs méthodes (H.4)
- Le token de validité persistant conditionné à la présence (H.4)

Cette combinaison offre le niveau de sécurité maximal : le dispositif est à la fois impossible à simuler (clé unique + comportement réactif) et impossible à transférer (invalidation dès détachement/éloignement).

Exemples de combinaisons sur dispositifs existants :
- Montre connectée avec PPG (pouls) + détection de bracelet fermé + token
- Téléphone avec détection de proximité d'un dispositif porté (UWB/Bluetooth vers montre, bracelet, ou autre) + accéléromètre
- Écouteurs avec détection de présence dans l'oreille + mouvement corrélé

Toute combinaison partielle ou totale des éléments décrits en H.1, H.2, H.3 et H.4 est couverte par la présente invention, que ce soit sur un dispositif dédié ou sur un produit grand public existant.

I) TECHNIQUES DE PIÉGEAGE ET VÉRIFICATION À RÉSULTAT ATTENDU :

Méthodes où l'entité de vérification connaît à l'avance le résultat attendu d'un test, permettant de détecter toute réponse simulée, falsifiée, ou issue d'un dispositif compromis. Ces techniques exploitent l'asymétrie d'information entre le vérificateur (qui connaît les résultats attendus) et un attaquant potentiel (qui ne peut que deviner).

I.1) Principe fondamental - Pièges à échec attendu :

L'entité de vérification peut envoyer des tests conçus pour ÉCHOUER dans certaines conditions. Un attaquant contrôlant le dispositif aura tendance à "corriger" ces échecs, se trahissant ainsi.

Fonctionnement :
- Certains tests sont conçus pour échouer dans la configuration actuelle
- Le serveur s'attend à cet échec et le considère comme un signe d'authenticité
- Un attaquant qui "fait réussir" un test censé échouer révèle la compromission
- Les proportions succès/échecs attendues sont inconnues de l'attaquant

I.2) Catégories de pièges (incluant, sans s'y limiter) :

A) PIÈGES MATÉRIELS (hardware) :
- Exploitation des caractéristiques physiques connues de l'appareil utilisé
- Le vérificateur connaît le modèle/marque exact des capteurs
- Comportements spécifiques attendus selon le hardware (bruit de fond caractéristique, latence native, distorsion optique, aberration chromatique)
- Signatures uniques du capteur (pattern de bruit, sensibilité spectrale)

B) PIÈGES TECHNIQUES :
- Exploitation des spécificités techniques de l'appareil
- Caractéristiques de la caméra (résolution, colorimétrie, compression)
- Comportements logiciels du firmware/OS
- Temps de réponse et latences caractéristiques du modèle
- Métadonnées et signatures numériques attendues

C) PIÈGES ALGORITHMIQUES :
- Tests dont le résultat attendu est calculé par le serveur
- Comportements logiciels spécifiques à vérifier
- Signatures algorithmiques des processeurs d'image de l'appareil
- Réponses attendues à des stimuli spécifiques
- Patterns statistiques connus pour le modèle d'appareil

I.3) Complexité statistique :

A) RÉSULTATS NON BINAIRES :
- Les tests ne produisent pas simplement "réussi/échoué"
- Chaque test génère un nuage de résultats probables selon la situation
- Le serveur connaît la distribution statistique attendue
- L'attaquant ne peut pas deviner quelle distribution est "normale"
- Toute déviation statistique significative indique une anomalie

B) CODE FRONTEND OPAQUE :
- Le code exécuté sur le dispositif ne révèle pas le résultat attendu
- Le code peut afficher un statut succès/échec destiné à tromper les attaquants basiques (faux indicateur, leurre)
- Le vrai verdict est calculé côté serveur avec des critères non divulgués
- Le système est conçu pour résister au reverse-engineering

I.4) Honeypot et étude des attaquants (optionnel) :

L'entité de vérification peut volontairement laisser passer certains spoofers détectés à des fins d'analyse :

Objectifs :
- Étudier les techniques d'attaque employées
- Accumuler des données sur les méthodes de falsification
- Construire une base de connaissance sur les attaquants
- Identifier et relier les tentatives d'attaque entre elles

Indicateur clé de spoofing :
- Un test conçu pour échouer dans certaines conditions
- Si ce test réussit SYSTÉMATIQUEMENT, même en conditions défavorables

- La "perfection suspecte" de l'attaquant le trahit

I.5) Avantage asymétrique :

Pour contourner ces pièges, un attaquant devrait :
- Connaître en détail le système de vérification (reverse-engineering complet)
- Connaître les caractéristiques exactes de l'appareil cible
- Connaître les proportions statistiques attendues pour chaque test
- Simuler de manière réaliste les échecs "naturels" attendus
- Maintenir cette simulation en temps réel sur tous les angles de capture

Cette combinaison de contraintes rend le contournement prohibitivement complexe, même pour un attaquant disposant d'un contrôle total (root) sur les dispositifs.

J) ANALYSE DE L'ÉCLAIRAGE CONTRÔLÉ ET CORRÉLATION DES ÉMISSIONS :

Technique exploitant les sources d'émission électromagnétique contrôlables par le système (incluant, sans s'y limiter : écrans, flashs, LEDs, projecteurs, lasers, émetteurs infrarouges, ou tout autre dispositif d'émission dans le spectre visible ou invisible) pour créer des effets observables et analysables sur la scène et les sujets capturés.

J.1) Principe fondamental :

Cette technique s'appuie sur les moyens d'émission commandables décrits indicativement en section 4.1.d), et décrit l'exploitation de leurs effets pour la vérification.

Toute source d'émission commandée par l'entité de vérification produit des effets observables et vérifiables :
- Éclairage direct de surfaces et objets (changement de luminosité, colorimétrie, ombres projetées)
- Réflexions spéculaires et diffuses sur les surfaces
- Réflexions sur les yeux, la peau, et autres surfaces réfléchissantes
- Ombres et pénombres créées par les objets de la scène
- Caustiques et effets de réfraction (à travers objets transparents)

J.2) Double corrélation multi-caméra :

Dans une configuration avec plusieurs caméras (intégrées ou sur dispositifs distincts), une source lumineuse commandée produit des effets capturables simultanément par plusieurs perspectives :

Exemple - Écran de smartphone comme source lumineuse :
- L'écran (face avant) émet des patterns lumineux commandés
- La caméra frontale capture les réflexions sur le visage de l'utilisateur
- La caméra arrière capture l'éclairage de la scène environnante
- La corrélation entre ces deux captures (reflets + éclairage) doit être cohérente avec la géométrie et les propriétés des surfaces
- Un simulateur devrait reproduire ces deux effets de manière parfaitement cohérente en temps réel, ce qui est extrêmement difficile

Exemple - Flash comme source ponctuelle :
- Le flash émet une impulsion lumineuse brève et intense
- Création d'ombres franches sur les surfaces (analysables géométriquement)
- Illumination du visage de l'utilisateur (analysable sur caméra frontale)
- La cohérence géométrique ombre/lumière entre les perspectives constitue un facteur de vérification
- Le timing précis de l'impulsion permet une synchronisation vérifiable

J.3) Patterns lumineux et séquences :

Le système peut commander des séquences lumineuses complexes :
- Variations de couleur (RGB, spectre complet)
- Variations d'intensité (pulses, gradients, patterns)
- Patterns spatiaux (formes, zones, balayages)
- Séquences temporelles (fréquences, rythmes, codes)

Ces patterns créent des signatures lumineuses analysables sur :
- Les surfaces de la scène (colorimétrie, luminosité)
- Les reflets cornéens (analyse des yeux)
- Les reflets cutanés (analyse de la peau)
- Les objets réfléchissants ou transparents de l'environnement

J.4) Sources d'émission couvertes (non limitatif) :

- Écrans (smartphones, tablettes, moniteurs, tout dispositif d'affichage)
- Flashs intégrés ou externes
- LEDs (intégrées ou accessoires)
- Projecteurs et sources de lumière ambiante contrôlable
- Lasers (si disponibles et sécurisés)
- Émetteurs infrarouges (invisibles mais détectables par certains capteurs)
- Tout autre dispositif capable d'émettre de l'énergie électromagnétique dans le spectre visible ou invisible, de manière contrôlée

J.5) Avantages de cette technique :

- Exploite des capacités matérielles déjà présentes sur la plupart des dispositifs (écran, flash)
- Ne requiert pas d'équipement supplémentaire
- Produit des effets physiques réels, difficiles à simuler
- Permet une vérification multi-angle avec un seul dispositif (caméras avant et arrière)
- Les effets sont vérifiables géométriquement et temporellement
- Combinable avec toutes les autres techniques de vérification

SYNTHÈSE ET PRINCIPE UNIFICATEUR

La présente section synthétise le principe fondamental de l'invention et établit son rôle unificateur vis-à-vis de l'ensemble des techniques décrites.

6.1 Principe fondamental - Détection d'incohérences multi-perspectives

Le cœur de l'invention repose sur le principe suivant :

Dès lors qu'une scène est observée depuis plusieurs perspectives distinctes, toute tentative de falsification doit maintenir une cohérence parfaite entre ces perspectives - cohérence qui est computationnellement prohibitive à simuler en temps réel.

Ce principe s'applique :

A) À DES PERSPECTIVES FRANCHEMENT DISTINCTES :
Plusieurs dispositifs physiquement séparés, chacun capturant la scène sous un angle différent.

B) À DES PERSPECTIVES OBTENUES PAR RÉFLEXION OU RÉTROACTION :
Un dispositif unique exploitant des surfaces réfléchissantes (miroirs, vitres, surfaces polies), des boucles optiques (mise en abyme), ou tout autre moyen permettant d'obtenir plusieurs perspectives d'une même scène à partir d'une source de capture unique ou d'un nombre réduit de sources.

C) À DES PERSPECTIVES MULTI-MODALES :
Différentes natures de capteurs (visuel, acoustique, thermique, télémétrique, inertiel) fournissant des "perspectives" complémentaires sur une même réalité physique.

Dans tous les cas, le principe reste identique : la cohérence entre les perspectives constitue la preuve d'authenticité, et l'incohérence constitue l'indicateur de falsification.

DÉFINITION - PERSPECTIVES DISTINCTES ET INDÉPENDANCE DE COMPROMISSION :

Une perspective est dite "distincte" ou "franchement différente" lorsque sa compromission ne peut être obtenue par la seule compromission d'un unique point du système. Cette distinction peut être :

A) NATURELLE (multi-dispositifs) :
Plusieurs appareils physiquement séparés constituent naturellement des points de compromission indépendants. La compromission d'un appareil ne compromet pas les autres.

B) CRÉÉE PAR DÉPENDANCE EXTERNE (mono-dispositif avec entité de vérification) :
Un appareil unique peut accéder à des perspectives "artificiellement distinctes" lorsque le flux de données transite par une entité externe (serveur, autre dispositif) qui :
- Contrôle les stimuli affichés (imprévisibles pour l'attaquant)
- Peut altérer, injecter, ou vérifier le flux de manière indépendante
- Rend impossible la pré-génération de réponses falsifiées cohérentes

Exemple : Un téléphone dont la caméra arrière capture, le flux transite par le serveur, puis est affiché sur l'écran avant, puis recapturé par la caméra frontale via un miroir. L'attaquant, même en compromettant

le téléphone, ne peut prédire ce que le serveur va injecter dans le flux retour, ni simuler la géométrie de la boucle optique en temps réel.

C) CRÉÉE PAR CONTRAINTES GÉOMÉTRIQUES VÉRIFIABLES :
Une boucle optique (miroir, mise en abyme) crée des relations géométriques entre les flux qui sont vérifiables par l'entité de vérification et impossibles à simuler par la seule manipulation logicielle locale.

La présente invention exploite ces trois modes, individuellement ou en combinaison, pour créer des perspectives dont la cohérence ne peut être falsifiée sans compromettre PLUSIEURS points indépendants du système (dispositifs ET/OU entité de vérification ET/OU contraintes physiques).

RENFORCEMENT CUMULATIF :

L'ensemble des perspectives distinctes, qu'elles soient naturellement ou artificiellement différentes, est destiné à être renforcé par les autres techniques de vérification décrites dans la présente demande, incluant, sans s'y limiter :

- Les techniques d'ancrage entropique (fluides, éléments chaotiques)
- Les techniques de boucle optique et mise en abyme
- Les défis physiques commandés par l'entité de vérification
- Les techniques de corrélation inertielle et positionnelle
- Les pièges algorithmiques et tests à échec attendu
- Toute autre technique décrite dans les sections 3, 4, et 5

Ces techniques s'appliquent de manière cumulative : chaque facteur de vérification supplémentaire MULTIPLIE la difficulté de falsification, créant un système où la compromission requiert de surmonter simultanément TOUS les facteurs actifs, et non chacun individuellement.

EXCLUSION - CE QUI N'EST PAS REVENDIQUÉ :

La simple combinaison de données multi-modales (visuel + profondeur, visuel + LIDAR, etc.) vérifiées LOCALEMENT sur un unique appareil, sans dépendance externe ni boucle de vérification, ne constitue PAS une mise en œuvre de l'invention. Ces configurations (incluant, sans s'y limiter : Apple Face ID, capteurs de profondeur Android, systèmes de reconnaissance faciale 3D intégrés) constituent un état de l'art existant où un unique point de compromission suffit à tromper l'ensemble du système.

6.2 Déclinaisons du principe

Ce principe fondamental se décline selon deux modes complémentaires :

A) MODE STATIQUE (sans mouvement des sources de capture) :
Analyse de la cohérence à un instant donné entre les perspectives capturées.
Cette analyse porte sur, incluant sans s'y limiter :
- Cohérence géométrique (angles, proportions, parallaxe)
- Cohérence photométrique (couleurs, luminosité, gradients)
- Cohérence radiométrique (distribution lumineuse, ombres, reflets)

- Cohérence télémetrique (distances, profondeurs)
- Cohérence topologique (relations spatiales entre éléments)

B) MODE DYNAMIQUE (avec mouvement d'une ou plusieurs sources de capture) :
Analyse de l'évolution cohérente des perspectives au cours du temps.
Cette analyse porte sur, incluant sans s'y limiter :
- Cohérence temporelle (synchronisation des changements observés)
- Cohérence cinématique (mouvements, vitesses, accélérations)
- Cohérence causale (relations cause-effet entre événements)
- Évolution cohérente de la géométrie lors des déplacements

Ces deux modes peuvent être utilisés séparément ou en combinaison, selon les besoins de la vérification et les capacités des dispositifs disponibles.

6.3 Relation avec les techniques décrites

L'ensemble des techniques décrites dans la présente demande (sections 3 et 4) constitue des applications, déclinaisons, ou exploitations spécifiques de ce principe unificateur. Notamment :

- Les techniques de stimulation (section 4.3.1.c) créent des conditions où les incohérences deviennent plus facilement détectables
- Les techniques de boucle de rétroaction (section 4.3.1.d) permettent d'obtenir des perspectives multiples avec un nombre réduit de dispositifs
- Les techniques d'ancrage entropique (section 4.3.1.e) introduisent des éléments dont la cohérence multi-perspectives est particulièrement difficile à simuler
- Les techniques biométriques multi-angles (section 3.3) appliquent le principe à la vérification d'identité humaine

Toute technique présente ou future exploitant la détection d'incohérences entre perspectives multiples - qu'elles soient spatiales, temporelles, modales, ou obtenues par tout autre moyen - relève du principe fondamental de l'invention.

6.4 Couverture étendue

La présente invention couvre :

- Toute configuration matérielle permettant d'obtenir plusieurs perspectives d'une même scène, qu'elle soit décrite explicitement dans ce document ou non

- Toute méthode d'analyse de cohérence entre perspectives, existante ou à venir

- Toute combinaison des techniques décrites, dans tout ordre et toute proportion

- Toute évolution technologique future permettant d'améliorer la détection d'incohérences ou d'augmenter le nombre/la qualité des perspectives capturées

- Toute application du principe à des domaines non explicitement mentionnés

Le principe unificateur de détection d'incohérences multi-perspectives constitue le fondement invariant de l'invention, indépendamment des évolutions technologiques des moyens de capture, de traitement, ou de falsification.

6.5 Protection des techniques individuelles et vision d'ensemble

A) SYSTÈME UNIFIÉ :

L'invention doit être considérée comme un système global unifié, où l'ensemble des techniques décrites peuvent être combinées pour atteindre le niveau de vérification maximal. La configuration optimale d'une session de vérification peut intégrer tout ou partie des techniques décrites, dans toute combinaison et toute séquence, selon les enjeux de sécurité et les ressources disponibles.

B) PROTECTION HIÉRARCHIQUE :

La présente demande vise à protéger :

1) EN PRIORITÉ : Le principe multi-perspectives dans son ensemble, tel que décrit en section 6.1, constituant le cœur de l'invention.

2) SUBSIDIAIREMENT : Chacune des techniques individuelles décrites dans le présent document, considérées séparément ou en sous-combinaisons, dès lors qu'elles présentent un caractère de nouveauté. Ces techniques incluent, sans s'y limiter :

- Les techniques de boucle de rétroaction et mise en abyme optique
- Les techniques d'ancrage entropique (fluides, éléments chaotiques)
- Les techniques de pièges algorithmiques à échec attendu
- Les techniques de stimulation exploitant les limitations de rendu
- La technique de l'image/frame en amont (requête prioritaire)
- L'utilisation d'objets physiques distincts à comportement vérifiable
- Les techniques de corrélation inertielle-visuelle
- Les techniques de reconstruction dynamique par mouvement
- Toute autre technique spécifiquement décrite dans le présent document

C) INDÉPENDANCE DES PROTECTIONS :

Chaque technique individuelle est revendiquée indépendamment de son intégration dans le système multi-perspectives. Une technique peut avoir une valeur protectrice propre même si elle est utilisée dans un contexte mono-dispositif ou hors du cadre du protocole complet.

D) CARACTÈRE ILLUSTRATIF ET NON LIMITATIF :

Les techniques individuelles sont décrites à titre illustratif pour supporter le principe unificateur. Leur description détaillée ne saurait limiter la portée de la protection du principe multi-perspectives, qui reste le fondement de l'invention. Inversement, si le principe multi-perspectives ne pouvait être protégé dans sa généralité, les techniques individuelles conservent leur vocation à être protégées séparément.

6.6 Clause de couverture étendue - Variantes architecturales et opérationnelles

NOTE DE CLARIFICATION - PORTÉE ET MODES DÉGRADÉS :

La présente section décrit les VARIANTES OPÉRATIONNELLES du système pour illustrer sa flexibilité et son adaptabilité. Il est important de distinguer :

(1) LES MODES PLEINEMENT COUVERTS PAR L'INVENTION (revendiqués comme nouveaux) :
- Architecture multi-dispositifs avec analyse corrélée externe
- Mono-dispositif avec dépendance externe (serveur, entité de vérification)
- Mono-dispositif avec techniques créant une distinction de perspectives (boucle optique, miroir, ancres d'entropie vérifiées par entité externe)

(2) LES MODES DÉGRADÉS / FALLBACK (décrits pour flexibilité, NON revendiqués comme innovants en eux-mêmes) :
- Vérification entièrement locale sans entité externe
- Mode offline sans synchronisation
- Dispositif agissant comme sa propre entité de vérification sans contrôle externe

Ces modes constituent un état de l'art existant ou des configurations de repli. Ils sont décrits pour assurer l'interopérabilité du système avec des environnements contraints, mais NE CONSTITUENT PAS le cœur de l'invention.

(3) LES TECHNIQUES PROTÉGÉES INDÉPENDAMMENT (annexes brevetables) :
Certaines techniques spécifiques décrites dans la présente demande sont protégées EN ELLES-MÊMES, indépendamment de l'architecture multi-perspectives. Cela inclut, sans s'y limiter :
- Les techniques de rétroaction visuelle et mise en abyme (section 3.3 J)
- Les techniques d'ancrage entropique par fluides/matériaux (section 3.3 I)
- Les techniques de corrélation inertielle et positionnelle (section 3.3 F)
- Les pièges algorithmiques et tests à échec attendu (section 5.7.I)

Ces techniques peuvent être appliquées même sur un mono-dispositif et constituent des innovations protégeables distinctes du principe multi-perspectives.

La présente invention couvre TOUTES les variantes architecturales et opérationnelles suivantes, qu'elles soient utilisées individuellement ou en combinaison, et quelle que soit la terminologie employée pour les désigner. Sauf indication contraire ci-dessous, ces variantes s'appliquent dans le cadre des modes (1) et (3) décrits ci-dessus :

A) VARIANTES DE L'ENTITÉ DE VÉRIFICATION :

L'entité de vérification peut être, sans s'y limiter :
- Un serveur distant (cloud, infrastructure dédiée, serveur tiers)
- Un serveur local (on-premise, réseau local, intranet)
- L'un des dispositifs de capture lui-même (mode maître) [MODE DÉGRADÉ - cf. (2)]
- Plusieurs dispositifs de capture agissant conjointement (mode coopératif)
- Une ressource de calcul distribuée entre dispositifs (mode réparti)
- Un dispositif tiers non impliqué dans la capture (arbitre externe)
- Une combinaison dynamique des éléments ci-dessus
- Toute entité capable d'effectuer l'analyse corrélée, quelle que soit sa

localisation physique ou logique

B) VARIANTES DE CONNECTIVITÉ :

Le système peut opérer :
- Avec connexion Internet permanente
- Avec connexion Internet intermittente
- Sans aucune connexion Internet (mode offline complet) [MODE DÉGRADÉ - cf. (2)]
- En connexion directe entre dispositifs (Bluetooth, WiFi Direct, NFC, ultrasons, infrarouge, câble, ou tout autre moyen de proximité)
- En mode mixte (certains dispositifs connectés, d'autres non)
- Avec synchronisation différée (vérification offline, validation ultérieure)
- Sans aucune synchronisation externe [MODE DÉGRADÉ si mono-dispositif - cf. (2)]
- Via réseaux mesh, ad-hoc, ou toute autre topologie de communication

C) VARIANTES DE CONTRÔLE :

Le contrôle du processus de vérification peut être :
- Centralisé (une entité unique décide)
- Décentralisé (consensus entre dispositifs)
- Distribué (responsabilités partagées)
- Hiérarchique (maître-esclave, coordinateur-participants)
- Pair-à-pair strict (aucune hiérarchie)
- Hybride (combinaison des modes ci-dessus)
- Dynamique (le mode de contrôle change au cours de la session)

D) VARIANTES DE CONFIANCE :

Les dispositifs participants peuvent être :
- Tous de confiance (appartenant au même propriétaire/opérateur)
- Partiellement de confiance (certains connus, d'autres non)
- Aucun de confiance (tous considérés comme potentiellement compromis)
- De confiance variable (niveau de confiance ajusté dynamiquement)
- Anonymes (identité des dispositifs non requise)
- Authentifiés (identité vérifiée par certificat, secret partagé, ou autre)

E) VARIANTES DE TEMPORALITÉ :

La vérification peut être :
- En temps réel strict (verdict immédiat requis)
- En temps réel souple (verdict dans un délai acceptable)
- Différée (analyse a posteriori)
- Asynchrone (chaque dispositif traite indépendamment)
- Par lots (accumulation puis traitement groupé)
- Continue (vérification permanente pendant toute la session)
- Ponctuelle (vérification à des instants spécifiques)
- Toute combinaison temporelle des éléments ci-dessus

F) VARIANTES GÉOGRAPHIQUES :

Les dispositifs peuvent être :
- Co-localisés (même pièce, même lieu)

- Proches (même bâtiment, même zone)
- Distants (localisations différentes)
- Mobiles (en déplacement pendant la vérification)
- Fixes (positions statiques)
- Toute combinaison de proximité et mobilité

G) VARIANTES DE PROPRIÉTÉ :

Les dispositifs peuvent appartenir :
- Au même utilisateur
- À des utilisateurs différents
- À des organisations différentes
- À des entités publiques
- À personne (dispositifs publics ou partagés)
- Être loués, empruntés, ou mis à disposition temporairement
- Toute combinaison de propriété

H) VARIANTES D'IMPLÉMENTATION :

Le système peut être implémenté :
- Entièrement en logiciel (application mobile, web, desktop)
- Entièrement en matériel (dispositifs dédiés)
- En combinaison matériel/logiciel
- Via firmware, microcode, ou logiciel embarqué
- Dans le cloud, en edge computing, ou localement
- De manière monolithique ou microservices
- Avec ou sans conteneurisation, virtualisation
- Sur tout système d'exploitation ou plateforme
- Toute architecture technique présente ou future

I) VARIANTES DE VERDICT :

Le résultat de la vérification peut être :
- Binaire (authentique/falsifié)
- Gradué (niveau de confiance, score, probabilité)
- Conditionnel (authentique sous réserve de...)
- Partiel (certains aspects vérifiés, d'autres non)
- Provisoire (sujet à révision ultérieure)
- Multiple (verdicts différents selon les critères)
- Explicatif (verdict avec justification détaillée)
- Opaque (verdict sans explication)

J) VARIANTES DE TRAITEMENT ET D'ANALYSE :

L'analyse de cohérence peut être effectuée par :
- Algorithmes déterministes (règles fixes, seuils)
- Intelligence artificielle (réseaux de neurones, ML, deep learning)
- Méthodes statistiques (distributions, corrélations)
- Analyse humaine (opérateur, expert, crowd-sourcing)
- Combinaison automatique/humaine (human-in-the-loop)
- Modèles pré-entraînés ou entraînés dynamiquement
- Heuristiques adaptatives

- Toute méthode computationnelle présente ou future

K) VARIANTES D'ÉCHELLE :

Le système peut impliquer :
- Deux dispositifs (configuration minimale)
- Trois à dix dispositifs
- Dizaines de dispositifs
- Centaines ou milliers de dispositifs (événements de masse)
- Un nombre variable de dispositifs au cours d'une même session
- Des dispositifs rejoignant ou quittant la session dynamiquement

L) VARIANTES DE DÉCLENCHEMENT :

La vérification peut être initiée par :
- L'utilisateur vérifié lui-même
- Un tiers demandant la vérification (banque, employeur, service)
- Le système automatiquement (déclenchement contextuel)
- Un événement externe (transaction, accès, alarme)
- Une programmation temporelle (vérifications périodiques)
- Une chaîne de vérifications (une vérification en déclenche une autre)
- Tout autre mécanisme de déclenchement

M) VARIANTES DE SUJET VÉRIFIÉ :

Le système peut vérifier :
- Une personne (identité, présence, vivacité)
- Un groupe de personnes
- Un objet (authenticité, intégrité, état)
- Un lieu ou une scène
- Un document ou un support d'information
- Un événement ou une situation
- Une transaction ou une action
- Un dispositif ou un équipement
- Toute entité ou situation observable par des capteurs

N) VARIANTES DE CAPTEURS :

Les sources de capture peuvent inclure, sans s'y limiter :
- Caméras (visible, infrarouge, UV, multispectrale, thermique)
- Microphones (audible, ultrasons, infrasons)
- Capteurs de profondeur (ToF, lidar, radar, stéréoscopie, lumière structurée)
- Capteurs inertiels (accéléromètre, gyroscope, magnétomètre)
- Capteurs de position (GPS, GNSS, UWB, triangulation)
- Capteurs biométriques (empreinte, iris, veine, voix)
- Capteurs environnementaux (température, pression, humidité, luminosité)
- Récepteurs radio (WiFi, Bluetooth, NFC, cellulaire, FM/AM, signaux ambiants)
- Capteurs chimiques ou olfactifs
- Tout capteur existant ou à développer

O) VARIANTES DE PERSISTANCE DES DONNÉES :

Les données de vérification peuvent être :
- Éphémères (supprimées immédiatement après vérification)
- Temporaires (conservées pour une durée limitée)
- Permanentes (archivées indéfiniment)
- Partiellement conservées (métadonnées sans données brutes)
- Hashées ou résumées (empreintes sans contenu original)
- Distribuées (fragments répartis, aucune entité n'a le tout)
- Chiffrées (accessibles uniquement sous conditions)
- Jamais transmises (vérification entièrement locale) [MODE DÉGRADÉ - cf. (2)]

P) VARIANTES D'INTÉGRATION :

Le système peut être intégré :
- En tant qu'application autonome (standalone)
- En tant que SDK/bibliothèque intégrée dans d'autres applications
- En tant qu'API appelable par des services tiers
- En tant que plugin/extension de navigateur ou plateforme
- En tant que service web (SaaS)
- En tant que fonctionnalité native du système d'exploitation
- En tant que firmware de dispositif dédié
- De manière invisible (intégré sans interface utilisateur dédiée)

Q) VARIANTES DE CONSENTEMENT ET PARTICIPATION :

La participation à la vérification peut être :
- Volontaire et explicite
- Requise par un service (condition d'accès)
- Transparente (l'utilisateur sait qu'il est vérifié)
- Discrète (vérification en arrière-plan avec consentement préalable)
- Incitative (récompenses pour participation)
- Obligatoire (contextes réglementés)
- Anonyme (vérification sans identification)
- Pseudonyme (identifiant non lié à l'identité réelle)

R) VARIANTES DE FALLBACK ET DÉGRADATION :

En cas de conditions sous-optimales, le système peut :
- Basculer vers un mode dégradé (moins de capteurs, tests simplifiés)
- Reporter la vérification (attente de meilleures conditions)
- Demander des actions compensatoires à l'utilisateur
- Accepter un niveau de confiance réduit
- Combiner avec d'autres méthodes de vérification (2FA, documents)
- Refuser la vérification (sécurité prioritaire)
- Opérer avec un sous-ensemble des dispositifs disponibles
- Toute stratégie d'adaptation aux contraintes

S) VARIANTES DE SECRET ET CONNAISSANCE :

Les informations peuvent être réparties ainsi :
- Secret total côté vérificateur (tests, critères, seuils inconnus)
- Secret partiel (certains éléments publics, d'autres non)
- Connaissance partagée (protocole public, paramètres secrets)

- Zero-knowledge (preuve sans révélation du contenu)
- Connaissance distribuée (aucune entité ne sait tout)
- Évolution du secret (rotation des clés, tests, paramètres)

T) VARIANTES D'ÉVOLUTION ET MISE À JOUR :

Le système peut évoluer :
- Par mise à jour logicielle des applications
- Par mise à jour des modèles d'IA côté serveur/entité
- Par mise à jour du protocole de vérification
- Par ajout de nouveaux types de tests
- Par adaptation automatique (apprentissage continu)
- Par configuration à distance (feature flags, paramètres)
- Sans aucune mise à jour des dispositifs (évolution côté entité seule)
- De manière transparente pour l'utilisateur

U) CLAUSE DE NON-LIMITATION ABSOLUE :

Toute variante, modification, adaptation, combinaison, permutation, ou évolution des éléments décrits dans la présente demande est couverte, incluant sans s'y limiter :

- Les variantes non explicitement mentionnées mais techniquement équivalentes
- Les variantes rendues possibles par des technologies futures
- Les variantes résultant de contraintes réglementaires, légales, ou pratiques
- Les variantes optimisées pour des cas d'usage spécifiques
- Les implémentations partielles du système (sous-ensembles fonctionnels)
- Les extensions du système (fonctionnalités additionnelles)
- Les adaptations à des contextes culturels, linguistiques, ou géographiques
- Toute mise en œuvre du principe fondamental multi-perspectives, quelle que soit la forme qu'elle prenne

Le silence de la présente demande sur un aspect particulier ne constitue pas une renonciation à la protection de cet aspect, dès lors qu'il découle du principe fondamental ou des techniques décrites.

La présente liste est donnée à titre illustratif et non limitatif. Toute variante, combinaison, ou évolution des éléments ci-dessus est couverte par l'invention dès lors qu'elle met en œuvre le principe fondamental de vérification multi-perspectives décrit en section 6.1.

L'absence de mention explicite d'une variante spécifique dans la présente demande ne saurait être interprétée comme une exclusion de cette variante du champ de protection de l'invention.

FIGURES (à joindre)

NOTE SUR LES FIGURES :
Les figures ci-dessous sont fournies à titre ILLUSTRATIF et NON LIMITATIF.

Elles représentent des modes de réalisation particuliers de l'invention et ne sauraient en aucun cas restreindre la portée de la protection aux seules configurations, proportions, dispositions, ou apparences représentées.

L'absence de représentation graphique d'un élément, d'une configuration, ou d'une variante décrite dans le texte ne constitue pas une exclusion de cet élément du champ de l'invention.

Les figures peuvent être complétées ou remplacées dans la demande définitive.

[Fig 1] Vue d'ensemble du dispositif de vérification multi-dispositifs

[Fig 2] Phase d'appairage par code visuel - scan du QR code


CTRL
FN
ALT
HDMI

[Fig 3] Phase de défis/instruction avec boucle de rétroaction optique visible

Revendications

Note préliminaire : À l'heure de ce dépôt, les revendications ci-dessous ne sont pas encore formulées selon le cadre réglementaire complet. Elles constituent une expression d'intention de protection.

INTENTION DE PROTECTION :

En premier lieu, l'inventeur entend revendiquer et protéger le concept de vérification de l'authenticité d'une scène, situation ou présence physique par l'utilisation de :
- plusieurs sources de capture,
- plusieurs natures de données,
- et surtout plusieurs perspectives et/ou plusieurs capteurs et/ou plusieurs dispositifs, apportant des perspectives différentes, ou franchement différentes,

ainsi que la vérification par perspective récursive (où une source de capture observe, directement ou indirectement, sa propre sortie visuelle, ou celle d'un autre appareil impliqué dans le processus de vérification).

De plus, l'inventeur entend protéger les techniques complémentaires mentionnées dans le présent document, incluant, sans s'y limiter, celles découlant de l'utilisation de plusieurs dispositifs, ou lorsqu'elles sont décrites dans un contexte mono-dispositif avec appareil ou équipement accessoire.

Plus largement, l'inventeur entend couvrir toute description technique et de procédé nouvelle ici présente, qu'elle soit liée ou indépendante de l'aspect multi-angle, dès lors que sa nouveauté serait attestée.

Cela inclut également toute solution de vérification basée sur l'utilisation d'une multiplicité d'appareils dans le cadre d'un processus anti-spoofing, non encore imaginée, déposée ou publiée à ce jour, tant que l'utilisation ou la nature de ces techniques relève du fait d'utiliser de multiples appareils de manière synchronisée et/ou unifiée dans le processus de vérification.

Techniques supplémentaires individuelles ayant vocation à être couvertes, incluant sans s'y limiter :
- La technique de l'image/frame en amont (éventuellement partielle, passée en requête prioritaire)
- L'objet distinct dédié à la vérification (identifiable individuellement, connu par l'entité de vérification)
- La rétroaction visuelle

NOTE SUR LA PORTÉE (SCOPE) :

L'invention vise en priorité les configurations multi-dispositifs (plusieurs appareils indépendants). Les configurations mono-dispositif (un seul appareil avec capteurs multiples) sont couvertes à titre de version dégradée ou de fallback du protocole, par exemple lorsque l'utilisateur ne dispose pas d'un second dispositif. Ces configurations mono-dispositif ne constituent pas le cœur de l'invention mais en sont des déclinaisons accessibles, en particulier lorsqu'il est possible à travers la configuration mono-dispositif d'accéder

à des perspectives différentes, ou franchement différentes (incluant, sans s'y limiter : double caméra avec flux passant par l'entité de vérification, affichage sur écran avec surface réfléchissante tierce, et défis de positionnement demandés à l'utilisateur exploitant les angles de réflexion).

CLARIFICATION - MONO-DISPOSITIF AVEC ÉLÉMENTS DISTINCTIFS :

Les configurations mono-dispositif sont couvertes par l'invention UNIQUEMENT lorsqu'elles intègrent une DÉPENDANCE EXTERNE créant une distinction de perspectives. Cette dépendance peut prendre la forme de :

- Transit du flux par une entité de vérification qui contrôle/vérifie
- Boucle optique dont la géométrie est vérifiée par l'entité
- Défis commandés par l'entité, imprévisibles pour l'attaquant
- Ancres d'entropie physiques dont le comportement est vérifié
- Toute autre technique rendant impossible la falsification locale seule

Ces éléments distinctifs peuvent être utilisés individuellement ou en combinaison cumulative pour renforcer la vérification. Plus le nombre de techniques actives est élevé, plus la difficulté de falsification augmente de manière multiplicative.

Sans cette dépendance externe, un système mono-dispositif multi-capteurs ne relève pas de la présente invention, quel que soit le nombre ou la diversité des capteurs intégrés.

Abrégé

L'invention concerne un système et procédé de validation de réalité physique utilisant une pluralité de sources de capture fournissant des perspectives différentes d'une même scène. Les données capturées sont analysées de manière corrélée par une entité de vérification pour vérifier leur cohérence géométrique, photométrique, radiométrique, télémetrique, et temporelle. Le système peut inclure des boucles de rétroaction optique entre dispositifs, l'introduction d'éléments physiques à haute entropie (fluides), et des mesures de latence. L'invention exploite le fait que la simulation convaincante d'une scène réelle sur plusieurs angles simultanément dépasse les capacités computationnelles actuelles, offrant ainsi une protection pérenne contre les tentatives d'usurpation.