RÉSUMÉ TECHNIQUE DES EXPOSÉS EN INVESTIGATION NUMÉRIQUE

NNA FRANCIS EMMANUEL ROMEO
Matricule : 22P056
Filière : CIN-4

Octobre 2025

— Synthèse technique et thématique —

1. Reconnaissance Faciale et Intelligence Artificielle

La reconnaissance faciale est une technologie biométrique issue de l'intelligence artificielle permettant d'identifier ou de vérifier une identité à partir des caractéristiques morphologiques du visage. Elle repose sur quatre modules principaux :

- **Acquisition** : capture d'images ou de flux vidéo à partir de capteurs.
- **Extraction de caractéristiques** : traitement d'images via CNN (Convolutional Neural Networks).
- **Correspondance** : comparaison des vecteurs de traits dans un espace euclidien ou cosinus.
- **Décision** : classification supervisée selon un seuil de similarité (θ).

Les approches actuelles combinent méthodes globales et locales via des architectures hybrides (FaceNet, ArcFace). Cette technologie joue un rôle clé dans les enquêtes forensiques et la surveillance intelligente.

2. Falsification de Messages Numériques et Chaîne de Preuve

Les échanges numériques (WhatsApp, Messenger, Telegram) constituent aujourd'hui des sources majeures de preuves judiciaires. Cependant, leur authenticité peut être compromise par :

- **Manipulation de captures d'écran** à l'aide d'outils comme Chatsmock, Photoshop ou HTMLForge.

— **Injection de faux messages** dans des bases SQLite d'applications mobiles.

Mesures préventives :

— Vérification des métadonnées et hachage (SHA-256).
— Corrélation entre horodatages et journaux système.
— Analyse de la signature numérique et de la source d'origine.
— Formation des magistrats et enquêteurs aux preuves numériques.

Ces étapes garantissent la traçabilité et l'intégrité de la preuve dans le respect du *Digital Evidence Standard* (Eoghan Casey).

3. Deepfake et Détection Forensique

Les **deepfakes** (faux profonds) exploitent des GANs (Generative Adversarial Networks) pour générer des vidéos ou audios ultra-réalistes.

— **Applications légitimes** : doublage automatique, accessibilité vocale, préservation patrimoniale.
— **Applications malveillantes** : usurpation d'identité, fraude vocale, désinformation.

Techniques de détection :

— Analyse spectrale et détection de jitter dans les signaux audio.
— Modèles de classification CNN-RNN entraînés sur DFDC et Celeb-DF.
— Intégration de filigranes numériques (watermarking quantique).

Le deepfake vocal illustre la convergence entre IA, cybersécurité et investigation numérique.

4. Archéologie des Régimes de Vérité Numérique

L'**archéologie numérique** foucaldienne analyse les discontinuités entre anciens et nouveaux régimes de vérité.

$$\vec{R_t} = (\alpha_T, \alpha_J, \alpha_S, \alpha_P)$$

— α_T : dominance technologique (plateformes, IA)
— α_J : dominance juridique (lois, RGPD)
— α_S : dominance scientifique (expertise, vérification)
— α_P : dominance politique/médiatique (influence, opinion)

De 1990 à 2020, la transition s'opère d'un régime *expert-centrique* vers un régime *plateforme-centré*, marqué par l'autorité algorithmique. Les discontinuités épistémologiques traduisent une **mutation socio-technique progressive mais disruptive**.

5. Cryptographie Post-Quantique et Protocole ZK-NR

Le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** vise à garantir la non-répudiation tout en préservant la confidentialité.

- **Architecture** : combinaison de Merkle Trees, signatures BLS à seuil et preuves STARKs.
- **Complexité** : génération de preuve $O(n \log n)$, vérification $O(1)$.
- **Sécurité** : résistance post-quantique (Dilithium, FALCON, SPHINCS+).

Ce modèle permet la vérification sans divulgation, ouvrant la voie à une nouvelle **chaîne de custody cryptographique** dans les enquêtes numériques modernes.

6. Cybercriminalité Africaine et Investigation Numérique

L'Afrique fait face à une explosion des menaces cybernétiques :

- **Ransomwares et fraudes bancaires** (Mobile Money, fintech).
- **Espionnage numérique étatique** et cyberactivisme.

Facteurs de vulnérabilité :

- Faible maturité législative et institutionnelle.
- Dépendance à l'hébergement étranger.
- Pénurie d'experts certifiés en forensic (moins d'un pour 100 000 hab.).

Méthodologie forensique standardisée :

1. Identification de l'incident.
2. Acquisition de preuves (images disques, journaux systèmes).
3. Préservation de l'intégrité (hachage, scellé numérique).
4. Analyse technique (Autopsy, FTK, Wireshark).
5. Rédaction du rapport et archivage probatoire.

7. Intelligence Artificielle Générative et Enjeux Probatoires

L'IA générative (ChatGPT, DALL·E, Synthesia) redéfinit la production de contenu et pose de nouveaux défis juridiques :

- **Traçabilité des modèles** : absence de logs explicites de génération.
- **Authenticité des preuves synthétiques** : difficulté à prouver la source.
- **Attribution** : nécessité de protocoles de marquage (watermark AI).

Les systèmes d'IA deviennent des **acteurs discursifs**, influençant la vérité numérique. D'où l'importance d'une approche *techno-éthique* de l'investigation numérique.

8. L'Investigation Numérique dans la Police Judiciaire Moderne

L'investigation numérique est aujourd'hui un pilier de la police judiciaire. Ses apports majeurs :

- **Récupération de traces invisibles** : fichiers supprimés, métadonnées, logs.
- **Reconstitution chronologique** : établissement de timelines précises.
- **Attribution des faits** : corrélation IP, journaux, signatures d'appareils.

Elle s'appuie sur la **méthodologie ACPO (Association of Chief Police Officers)** :

1. Ne jamais altérer les données originales.
2. Documenter toute action effectuée.
3. Maintenir la chaîne de custody.
4. Garantir la reproductibilité des analyses.

L'investigation numérique devient ainsi une **science probatoire** au cœur de la justice digitale.

— Fin du résumé technique des exposés —