RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE
****
DÉPARTEMENT DE GENIE INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
****
DEPARTMENT OF COMPUTER ENGINEERING
****

RESUME EXPOSES
INVESTIGATION NUMERIQUE

Option :

Cybersécurité et Investigation Numérique

Rédigé par :
GHOUMO DONFACK OLIVIA, *22P023*

Sous l'encadrement de :
M. Thierry MINKA

Année académique 2025 / 2026

TABLE DES MATIÈRES

I Reconnaissance Faciale : Algorithmes et Enjeux

I.1 Contexte et objectifs

Ce document présente une analyse approfondie des algorithmes de reconnaissance faciale dans le contexte de l'investigation numérique. Il explore les fondements techniques, les applications pratiques et les enjeux éthiques et juridiques de cette technologie biométrique.

I.2 Présentation technique

La reconnaissance faciale fonctionne selon trois phases principales : l'enrôlement (capture et stockage des caractéristiques faciales), l'identification (recherche 1-N dans une base de données) et la vérification (comparaison 1-1 pour confirmer une identité). L'architecture système comprend quatre modules essentiels : capture/acquisition, extraction de caractéristiques, correspondance et décision.

Les méthodes de reconnaissance se divisent en trois catégories : les méthodes globales (PCA, LDA, SVM) qui analysent l'ensemble du visage, les méthodes locales (HMM, EBGM) qui se concentrent sur des régions spécifiques, et les méthodes hybrides combinant plusieurs approches. Des détecteurs comme SIFT, HOG et SURF permettent d'identifier et de décrire les points d'intérêt dans les images faciales.

I.3 Avantages et limites

Les points forts incluent l'automatisation rapide de l'identification sur de vastes volumes de données visuelles, essentielle pour les enquêtes judiciaires. Cependant, plusieurs faiblesses critiques sont identifiées : l'architecture "boîte noire" des modèles deep learning complique leur traçabilité, les performances chutent en conditions réelles (faible luminosité, angles extrêmes), et l'interopérabilité entre systèmes reste problématique.

Sur le plan sécuritaire, les systèmes sont vulnérables aux attaques adversariales, deepfakes et manipulations diverses. Les données biométriques, une fois compromises, ne peuvent être modifiées comme un mot de passe. Les enjeux éthiques sont majeurs : atteintes à la vie privée, biais algorithmiques envers certaines populations, effet dissuasif sur les libertés publiques.

I.4 Recommandations pour le Cameroun

Le document propose un cadre d'encadrement rigoureux adapté au contexte camerounais. Sur le plan technique, il recommande de documenter intégralement le pipeline, réaliser des tests locaux sur des jeux de données représentatifs et combiner modèles profonds avec descripteurs classiques.

Pour la sécurité, des pentests réguliers incluant des attaques adversariales sont nécessaires, avec protection cryptographique des templates biométriques et mécanismes anti-spoofing multi-sensoriels. L'aspect éthique requiert des études d'impact (DPIA), des audits de biais et des mécanismes de recours pour les citoyens.

La conformité juridique doit s'aligner sur la loi n°2024/017 sur les données personnelles, avec base légale claire (mandat judiciaire, consentement), enregistrement auprès de l'ANPD et limitation des usages sensibles. Aucune décision critique ne doit reposer uniquement sur un résultat automatique sans validation humaine.

I.5 Conclusion

La reconnaissance faciale constitue un outil puissant mais à double tranchant pour l'investigation numérique. Sans encadrement rigoureux, elle peut générer des dérives graves. Sa mise en œuvre au Cameroun nécessite un cadre juridique actualisé, une supervision technique continue et une utilisation proportionnée pour concilier sécurité et respect des droits fondamentaux.

II L'Investigation Numérique dans la Police Judiciaire

II.1 Problématique et apports essentiels

Ce travail analyse l'utilité de l'investigation numérique (digital forensic) pour la police judiciaire camerounaise face à la criminalité moderne. L'investigation numérique consiste à collecter, analyser et présenter des preuves issues de supports électroniques pour appuyer les enquêtes.

Les apports sont multiples : accès à des preuves invisibles dans le monde physique (historiques, métadonnées, fichiers supprimés), lutte efficace contre la cybercriminalité, identification et traçage des auteurs via adresses IP et géolocalisation, reconstitution chronologique des événements numériques, et production de preuves recevables en justice.

II.2 Domaines d'application au Cameroun

La lutte contre la cybercriminalité inclut le démantèlement de réseaux de fraude en ligne. En 2022, un réseau basé à Douala fut démantelé grâce à l'analyse des transactions et logs de connexion. La Gendarmerie nationale utilise ces techniques contre le phishing ciblant les entreprises camerounaises.

Pour la criminalité transfrontalière et le terrorisme, Interpol Cameroun a identifié des réseaux de trafic de stupéfiants Nigeria-Cameroun via l'analyse de données téléphoniques. Dans la lutte contre Boko Haram, l'extraction de messages a permis de cartographier les réseaux logistiques et d'anticiper des attaques.

La criminalité financière fait l'objet d'investigations via le traçage de transactions électroniques. En 2021, un réseau de détournement de fonds publics fut démantelé après analyse de fichiers administratifs et comptes bancaires. Les crimes violents (kidnappings, vols) bénéficient de l'analyse des téléphones et vidéosurveillance pour reconstituer les événements.

La protection de l'enfance mobilise ces techniques pour démanteler les réseaux de pédopornographie. En 2022, le Commissariat central de Yaoundé neutralisa un réseau grâce à la collaboration avec Interpol et Europol.

II.3 Outils et techniques

Les logiciels de récupération incluent Autopsy, FTK Imager et Cellebrite pour restaurer données supprimées et analyser métadonnées. Les outils mobiles spécialisés comme Oxygen Forensic Detective extraient les données des smartphones.

Pour l'investigation réseau, Wireshark analyse le trafic, tandis que des outils surveillent le dark web. La lutte contre le chiffrement mobilise des techniques de cryptanalyse et craquage de mots de passe (Hashcat) sous ordonnance judiciaire.

II.4 Défis et limites camerounais

Le volume exponentiel de données (smartphones de 128GB+) et la diversité des formats nécessitent des outils spécialisés. Une analyse forensic complète peut prendre plusieurs semaines. L'équilibre entre investigation et respect de la vie privée (Article 9 Constitution) exige des mandats conformes à la loi cybersécurité 2010.

L'obsolescence rapide des technologies nécessite une formation continue coûteuse. Le Cameroun souffre d'une pénurie d'experts (moins de 50 experts certifiés), concentrés à Yaoundé et Douala. Les équipements coûteux (station forensic à 25 millions FCFA) et budgets insuffisants limitent les capacités opérationnelles.

Les difficultés juridiques incluent les risques de rejet des preuves si la chaîne de custody n'est pas respectée, et l'absence de standards clairs pour l'admissibilité des preuves électroniques.

II.5 Perspectives

L'investigation numérique s'impose comme un pilier fondamental de toute enquête criminelle moderne. Le Cameroun doit investir dans la formation continue, le renforcement logistique des unités spécialisées et l'adaptation du cadre juridique. Les défis futurs incluent l'intelligence artificielle, le métavers criminel, les deepfakes et l'ère post-quantique, nécessitant une anticipation stratégique pour la souveraineté numérique nationale.

III Logiciels de Rédaction de Mémoire

III.1 Contexte et enjeux

Ce document de analyse trois outils majeurs pour la rédaction académique : Overleaf, Microsoft Word et Zotero. Le choix des outils logiciels devient déterminant pour la réussite d'un mémoire, devant répondre à plusieurs impératifs : environnement adapté aux longs documents, gestion rigoureuse des références bibliographiques et mise en forme selon les standards académiques.

III.2 Overleaf : excellence académique par LaTeX

Fondé en 2012 par deux mathématiciens et racheté en 2023 par Springer Nature, Overleaf est un éditeur LaTeX en ligne collaboratif devenu standard dans l'édition scientifique. Sa philosophie repose sur l'accessibilité (usage sans installation complexe), la collaboration (travail d'équipe synchronisé) et la qualité (standards professionnels).

Les atouts majeurs incluent une qualité typographique exceptionnelle avec placement optimal des figures et justification parfaite, une gestion avancée des références croisées avec numérotation automatique, une collaboration en temps réel avec historique des modifications, et une bibliothèque de templates académiques conformes aux exigences universitaires.

Les limites concernent la courbe d'apprentissage élevée pour les non-initiés à LaTeX, l'édition hors ligne limitée en version gratuite, et une interface moins intuitive que les traitements de texte classiques pour les corrections rapides. Des alternatives existent : LyX (interface simplifiée), TeXmaker et TeXstudio (éditeurs locaux), Authorea (plateforme collaborative).

III.3 Microsoft Word : référence universelle

Word détient une position hégémonique par son intégration à Microsoft Office, son interface familière et sa compatibilité quasi universelle (format .docx). Pour les mémoires, il offre une gestion avancée des styles hiérarchiques, une génération automatique des tables (matières, figures, tableaux), un suivi des modifications efficace pour les échanges avec le directeur, et une compatibilité facilitant les échanges.

Les inconvénients incluent une gestion bibliographique native limitée, des risques d'instabilité sur documents volumineux (ralentissements, corruption), et une approche visuelle potentiellement peu structurante sans usage rigoureux des styles. Les alternatives sont LibreOffice Writer (gratuit) et Google Docs (collaboration cloud).

III.4 Zotero : spécialiste bibliographique

Zotero est un gestionnaire de références open-source développé par l'Université George Mason, incarnant une vision démocratique de la gestion bibliographique. Il permet de centraliser, organiser et exploiter toutes les sources d'un mémoire.

Les fonctionnalités essentielles incluent la capture automatique intelligente des métadonnées depuis catalogues et bases scientifiques, l'intégration transparente avec Word et LibreOffice via plugins, la gestion de milliers de styles de citation (APA, MLA, Chicago, Vancouver), et la synchronisation cloud avec stockage des PDF.

L'écosystème s'enrichit d'extensions comme ZotFile (gestion PDF) et Better BibTeX (pour LaTeX). Les alternatives sont Mendeley (propriétaire Elsevier), EndNote (professionnel payant) et Citavi (gestion complète avec planification).

III.5 Combinaisons optimales

Le duo Word + Zotero convient à la majorité des étudiants, offrant accessibilité et rigueur bibliographique. La triade Overleaf + Zotero + ZoteroBib représente l'excellence académique pour travaux exigeants. Le workflow Overleaf + Zotero Groups est idéal pour la collaboration.

Les recommandations par profil suggèrent Word + Zotero pour les débutants, Overleaf + Zotero pour les scientifiques maîtrisant LaTeX, et Overleaf + Zotero Groups pour les projets collaboratifs et thèses.

III.6 Conclusion

La réussite d'un mémoire repose sur le choix stratégique d'outils complémentaires. Overleaf excelle en qualité typographique, Word en accessibilité, Zotero en rigueur bibliographique. La combinaison Overleaf + Zotero offre le meilleur équilibre qualité-efficacité. Cependant, ces outils restent des instruments au service de la pensée : la perfection technique ne doit pas occulter la substance intellectuelle et la profondeur de la recherche.

IV Simulation de Falsification de Messages WhatsApp

IV.1 Objectif pédagogique

Ce travail illustre les possibilités techniques de falsification de preuves numériques via la simulation d'échanges WhatsApp entre un enseignant (Paul KENGNE) et une étudiante, dans le cadre d'une relation extra-conjugale fictive. L'objectif est d'illustrer les capacités techniques de manipulation et de questionner la fiabilité des preuves numériques en investigation.

IV.2 Méthodologie de falsification

Deux outils principaux ont été mobilisés. Chatsmock, application web, permet de créer de fausses conversations WhatsApp réalistes en définissant les participants (noms, photos, numéros), en générant des messages avec contenu libre, en paramétrant heure, date et statut de lecture, et en produisant des captures d'écran identiques à l'application réelle.

Adobe Photoshop a ensuite affiné le réalisme en corrigeant les détails graphiques (alignement, bulles, icônes), en modifiant ou insérant des éléments supplémentaires (images envoyées), et en retouchant l'interface pour correspondre parfaitement à un smartphone réel. Cette association démontre la simplicité technique de fabriquer de fausses preuves numériques.

IV.3 Scénario simulé

Sept captures d'écran et deux photos ont été produites, révélant des propos à caractère affectif et sexuel explicite, des invitations hors cadre scolaire, des expressions comme "Bonsoir mon cœur", "ma femme est une folle", "Je t'aime mon sucre", et des promesses de quitter l'épouse. Ce contenu illustre un cas typique de manipulation potentielle dans un contexte disciplinaire ou judiciaire.

IV.4 Limites et comparaison d'outils

Chatsmock présente des limites : manque de réalisme sur certains détails récents de WhatsApp, fonctionnalités restreintes (difficile de simuler notes vocales, appels), dépendance au format image, et détection possible par analyse forensique des métadonnées et anomalies graphiques.

Les alternatives incluent FakeChat (plus d'options visuelles mais moins crédible), WhatsFake (usage ludique, interface moins personnalisable), Photoshop (liberté totale, réalisme indétectable mais compétences requises), et détournement d'outils forensiques pour injection directe dans les bases de données.

IV.5 Impact sur l'investigation numérique

L'accessibilité de ces outils pose des défis majeurs : baisse de la fiabilité des captures d'écran comme preuves irréfutables, difficultés accrues pour les experts forensiques, risques de manipulation judiciaire ou disciplinaire pour nuire à autrui, et multiplication des faux dossiers compliquant le travail institutionnel.

IV.6 Recommandations pratiques

Face à ces risques, plusieurs mesures sont proposées : vérification technique des métadonnées (horodatage, signature numérique, origine) pour confirmer l'authenticité, sensibilisation des acteurs judiciaires à la reconnaissance des falsifications, utilisation d'outils spécialisés de détection de

manipulations d'images, préférence pour la récupération directe depuis les bases de données plutôt que captures d'écran, et renforcement du cadre légal sur l'acceptabilité des preuves numériques.

IV.7 Conclusion

Cette expérience démontre la simplicité de créer des preuves numériques trompeuses, révélant la fragilité des éléments issus de messageries instantanées. Elle illustre un double constat : les menaces pour la crédibilité des investigations, et la nécessité d'adopter des méthodes de vérification rigoureuses. L'investigation numérique doit intégrer des techniques avancées de vérification et une sensibilisation accrue pour garantir l'intégrité des preuves dans un monde où la manipulation devient accessible.

V Les Dix Cas Majeurs de Hacking en Afrique

V.1 Contexte et méthodologie

Ce document analyse dix cas emblématiques de cyberattaques en Afrique entre 2015 et 2025, période marquée par une augmentation de trois cent pourcent des incidents selon Interpol, avec plus de trois mille attaques hebdomadaires par organisation. Cette analyse s'appuie sur quatre critères d'évaluation : la taille de l'attaque (étendue, durée, complexité), le type d'organisation visée, le volume de données affectées, et les conséquences financières et réputationnelles.

V.2 État de la cybersécurité africaine

La vulnérabilité du continent s'explique par plusieurs facteurs structurels. La faible maturité institutionnelle se manifeste par l'absence de législations complètes en cybersécurité dans la plupart des États. Le manque de compétences locales est criant, avec moins d'un expert pour cent mille habitants. Les infrastructures obsolètes reposent sur des logiciels non mis à jour, tandis que la dépendance extérieure se traduit par l'hébergement des données hors du continent.

Les principales menaces observées incluent les ransomwares qui chiffrent les données contre rançon, les fraudes au mobile money et systèmes bancaires, l'espionnage numérique à fins politiques, les attaques par déni de service contre plateformes publiques, et les campagnes de désinformation. Cependant, une dynamique positive émerge : le Maroc, le Nigeria, l'Afrique du Sud et le Cameroun se dotent progressivement de centres de réponse aux incidents, de législations cybernétiques et de formations spécialisées.

V.3 Méthodologie d'investigation

L'investigation numérique s'articule autour de cinq étapes fondamentales. L'identification de l'incident détecte précocement l'attaque et définit son périmètre. La collecte des preuves acquiert les données depuis disques, serveurs, journaux et réseaux. La préservation de l'intégrité réalise des copies forensiques avec hachage et stockage sécurisé. L'analyse technique mobilise des outils spécialisés comme Autopsy, FTK, EnCase et Wireshark. La rédaction du rapport documente rigoureusement les conclusions pour les juridictions et décideurs.

V.4 Cas majeurs analysés

Le ransomware sur Transnet en Afrique du Sud en juillet 2021 illustre l'attaque d'infrastructures critiques. Le groupe BlackMatter a paralysé les opérations portuaires et ferroviaires, chiffrant plus de sept téraoctets de données logistiques et systèmes ERP. L'impact financier atteint soixante millions de dollars avec trois semaines d'arrêt partiel des ports de Durban, Cape Town et Ngqura.

Le breach de la CNSS marocaine en avril 2025 constitue une atteinte massive aux données personnelles. Deux millions de salariés et cinq cent mille entreprises ont vu leurs informations exfiltrées, incluant numéros d'identification, salaires et historiques médicaux. L'attaque, revendiquée par un groupe se présentant comme algérien, a révélé l'absence de chiffrement des données sensibles, entraînant une perte de confiance institutionnelle majeure.

L'attaque sur Eneo Cameroun en janvier 2024 a perturbé les services informatiques du fournisseur national d'électricité, affectant particulièrement les clients prépayés et compteurs intelligents. Les systèmes de facturation et services de paiement en ligne ont été compromis, avec des pertes estimées à plusieurs centaines de millions de francs CFA.

L'attaque GhostLocker 2.0 en Égypte en 2024 a ciblé trente organisations industrielles et gouvernementales. Cette variante évoluée de ransomware du collectif GhostSec a combiné vol et chiffrement de données, exigeant vingt millions de dollars de rançon. Elle a exposé la vulnérabilité des États africains en transformation numérique face aux cybercriminels transnationaux.

Le scandale Pegasus au Maroc entre 2020 et 2021 illustre l'espionnage numérique sophistiqué. Ce logiciel espion a ciblé journalistes, militants et opposants politiques, soulevant des questions majeures sur la surveillance gouvernementale et le respect des droits humains dans le cyberespace africain.

Le piratage des banques ivoiriennes a visé simultanément UBA, BNI et NSIA Bank, compromettant données clients, identifiants bancaires et transactions SWIFT. Les pertes directes de six millions d'euros résultent d'une campagne de phishing ciblant les cadres bancaires et l'utilisation de Remote Access Trojans, démontrant que la cybersécurité humaine reste le maillon faible.

La cyberattaque sur les systèmes de santé tunisiens en 2021 a combiné attaque DDoS et ransomware contre le Ministère de la Santé et hôpitaux publics. Les dossiers médicaux numériques et serveurs hospitaliers ont été compromis, retardant des traitements critiques et causant deux millions et demi de dollars de pertes. Cet incident souligne l'importance cruciale de la cybersécurité sanitaire.

Le piratage d'Ethiopian Airlines en 2023 a compromis mondialement le système de réservation de la compagnie nationale, exposant les données personnelles de milliers de passagers. Les indemnités et atteinte réputationnelle sont estimées à cinq millions de dollars, illustrant les risques de cyber-espionnage industriel dans le transport aérien.

La fraude au Mobile Money MTN Nigeria en 2018 a détourné environ huit millions de dollars en exploitant des failles dans les API et bénéficiant de complicités internes. Ce réseau touchant plusieurs millions d'utilisateurs a conduit MTN à introduire l'intelligence artificielle dans la détection des transactions anormales.

Le piratage de la Banque Centrale du Nigeria entre 2015 et 2016 constitue une intrusion prolongée sur les serveurs SWIFT. Cette attaque menée par un groupe international a compromis données financières et courriers internes, nécessitant l'intervention conjointe du FBI et d'Interpol. Elle a déclenché une refonte complète du système de sécurité bancaire national avec des pertes de plusieurs dizaines de millions de dollars.

V.5 Recommandations stratégiques

Sept axes d'amélioration sont proposés pour renforcer la cybersécurité africaine. La formation massive d'experts en cybersécurité et forensic numérique doit devenir prioritaire. La création de CERT/CSIRT régionaux capables d'échanger en temps réel sur les menaces permettra une réponse coordonnée. L'harmonisation des lois africaines autour de la Convention de Malabo établira un cadre juridique cohérent.

Le développement d'un hébergement local et d'un cloud souverain africain réduira la dépendance extérieure. Le renforcement de la gouvernance numérique dans les entreprises publiques améliorera la résilience institutionnelle. Les audits réguliers de sécurité et la sensibilisation des employés préviendront les attaques exploitant le facteur humain. Enfin, la mise en place de fonds de cyber-résilience aidera les PME à se protéger.

V.6 Conclusion

L'Afrique se trouve à un carrefour stratégique où son avenir numérique dépend de sa capacité à sécuriser ses infrastructures et former ses talents. Les dix cas analysés démontrent que les attaques

ne sont pas isolées mais révèlent une transformation profonde du paysage cybercriminel continental. La cybersécurité doit être considérée comme une responsabilité partagée entre institutions publiques, entreprises privées et citoyens. Renforcer les capacités d'investigation numérique et bâtir une souveraineté technologique constituent les conditions indispensables pour un développement numérique durable et sécurisé du continent africain.

VI Deepfake Vocal : Enjeux et Investigation

VI.1 Introduction au phénomène

Ce rapport explore le deepfake vocal, forme particulièrement préoccupante de manipulation audio utilisant l'intelligence artificielle. Cette technologie reproduit ou imite de façon quasi indiscernable la voix humaine grâce à des modèles entraînés sur des enregistrements réels, générant des discours jamais prononcés par la personne imitée à partir de quelques secondes d'échantillons.

VI.2 Évolution historique

L'évolution des deepfakes audio suit une trajectoire marquée par plusieurs périodes clés. De 1930 à 1990, la naissance des reproductions vocales voit le Voder de Bell Labs en 1939 comme première machine électronique produisant de la parole, suivie par les vocoders et synthèse par concaténation des années 1960 à 1990, produisant des voix encore robotiques.

La période 2000 à 2015 marque l'évolution statistique avec le passage aux modèles HMM paramétriques, plus naturels mais encore artificiels. La révolution du deep learning survient en 2016 avec WaveNet de DeepMind, produisant des ondes audio réalistes et marquant le vrai tournant de la synthèse vocale neuronale.

Entre 2016 et 2017, les démonstrations publiques se multiplient avec Adobe Project VoCo permettant d'éditer et cloner une voix, et Lyrebird promettant le clonage vocal avec peu de données, engendrant les premiers débats éthiques. La démocratisation s'impose entre 2017 et 2020 avec des modèles comme Tacotron et Deep Voice, et des outils open-source permettant le clonage vocal en quelques secondes.

Depuis 2019, l'usage malveillant émerge avec la première fraude connue en 2019 utilisant la voix deepfake d'un PDG pour escroquer une entreprise. Depuis 2023-2024, la multiplication d'arnaques et usurpations d'identité par téléphone et messagerie s'accélère.

VI.3 Contextes d'utilisation

Les applications légitimes incluent l'accessibilité pour personnes ayant perdu l'usage de la parole (patients atteints de SLA, laryngectomisés), le doublage multilingue accéléré de films sans dénaturer le jeu d'acteur, les assistants virtuels avec interactions plus naturelles, et la préservation des voix d'artistes ou proches disparus à fins mémorielles.

Les applications malveillantes englobent les escroqueries financières par imitation de responsables hiérarchiques pour obtenir des transferts d'argent, l'usurpation d'identité contournant les systèmes d'authentification vocale, la manipulation de l'opinion publique par diffusion de faux discours, et la falsification de preuves numériques dans enquêtes ou procès.

VI.4 Enjeux pour l'investigation numérique

L'atteinte à la fiabilité des preuves audio menace le triptyque CRO. La confidentialité est compromise par les enregistrements vocaux clonés diffusés sans autorisation, exposant des données sensibles. La fiabilité est fragilisée car l'introduction de contenus falsifiés remet en question l'authenticité des preuves audio et leur valeur probante. L'opposabilité devient problématique si l'on ne peut démontrer qu'un enregistrement est exempt de manipulation.

La complexification de la vérification impose que l'analyse forensique audio intègre désormais des techniques d'intelligence artificielle capables de repérer signatures et artefacts subtils liés à la

synthèse vocale. La transparence des méthodes et outils devient indispensable pour l'acceptation judiciaire des résultats.

La nécessité de comprendre le fonctionnement technique (réseaux neuronaux, vocodeurs, spectrogrammes, empreintes acoustiques) devient cruciale pour détecter les falsifications, expliquer clairement les conclusions devant un tribunal et anticiper les nouvelles formes d'attaques audio.

VI.5 Cas pratique MINIMAX audio

MINIMAX audio est une technologie basée sur l'intelligence artificielle spécialisée dans la synthèse et transformation de la voix humaine. Elle utilise des modèles entraînés sur vastes bases de données vocales pour imiter précisément timbre, intonation et rythme d'un locuteur réel, proposant des applications dans le divertissement, l'éducation et l'accessibilité numérique.

L'utilisation pratique démontre la facilité de création de deepfakes vocaux. Le processus commence par l'accès à la plateforme en ligne via un compte créé avec messagerie temporaire. La fonctionnalité Voice Clone permet de charger la voix d'une personne pour créer un clone vocal. La fonction Text To Speech utilise ensuite ce clone pour faire dire des phrases jamais prononcées. Le Voice Isolator supprime le bruit pour améliorer la qualité.

Les résultats obtenus sont d'un réalisme impressionnant, rendant la détection presque impossible à l'oreille humaine. Cette démonstration illustre l'accessibilité inquiétante de technologies de manipulation vocale sophistiquées.

VI.6 Risques et cas réels

Les risques englobent plusieurs dimensions. Sur le plan sécuritaire, l'usurpation vocale facilite fraude et chantage. Les impacts sociaux et psychologiques incluent atteintes à la réputation.

VII Deepfake Vidéo : Génération par Intelligence Artificielle

VII.1 Introduction et contexte

Ce travail explore la réalisation d'un deepfake pédagogique utilisant GPT-5 pour la rédaction du script et HeyGen pour la génération vidéo. L'émergence de l'intelligence artificielle générative a profondément transformé les pratiques de création de contenus numériques, offrant de nouvelles possibilités dans la communication, la pédagogie, le divertissement et la recherche.

L'association des modèles de langage capables de produire des scripts structurés et cohérents avec les plateformes de synthèse vidéo spécialisées dans la génération de visuels réalistes constitue un axe d'expérimentation particulièrement prometteur. Ce projet illustre concrètement comment l'intelligence artificielle peut être mise au service de la production de contenus immersifs, tout en soulevant des questions éthiques et méthodologiques.

VII.2 Concept du deepfake

Un deepfake est un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle. Ce terme, abréviation de "Deep Learning" et "Fake" (fausse profondeur), fait référence à des contenus faux rendus profondément crédibles par l'intelligence artificielle.

En 2014, le chercheur Ian Goodfellow inventa la technique GAN (Generative Adversarial Networks) à l'origine des deepfakes. Selon cette technologie, deux algorithmes s'entraînent mutuellement : l'un tente de fabriquer des contrefaçons aussi fiables que possible, l'autre tente de détecter les faux. De cette façon, les deux algorithmes s'améliorent ensemble au fil du temps grâce à leur entraînement respectif.

Les inconvénients liés aux deepfakes sont nombreux : manipulation de l'information, atteintes à la réputation, usurpation d'identité, fraudes diverses et risques pour la démocratie. L'avenir des deepfakes passe par le développement de contre-mesures. Le laboratoire FAIR de Facebook travaille sur un projet de "désidentification" avec des filtres empêchant l'exploitation par des logiciels de reconnaissance faciale. Depuis novembre 2019, la CNIL manifeste sa volonté de créer un cadre législatif et réglementaire pour la reconnaissance faciale et la conception des deepfakes.

VII.3 Présentation des outils

HeyGen AI est une intelligence artificielle spécialisée dans la génération de vidéos par IA, créée en 2022. Cet outil se distingue par sa capacité à transformer de simples instructions textuelles en séquences audiovisuelles captivantes, sans exiger de matériel sophistiqué ni de compétences techniques avancées. Son accessibilité et sa rapidité d'exécution ouvrent un large éventail de possibilités pour professionnels et particuliers.

Les utilisations de HeyGen incluent la création de contenu et le journalisme pour diffuser actualités ou histoires avec impact visuel fort, la communication d'entreprise pour présenter produits ou services de façon professionnelle, et l'enseignement et formation pour transformer des cours en expériences interactives et engageantes adaptées aux nouvelles pratiques d'apprentissage.

GPT-5, développé par OpenAI et sorti le 7 août 2025, est le premier modèle d'IA "unifié" combinant les capacités de raisonnement de la série o aux possibilités de réponses rapides de la série GPT. C'est un pas vers des systèmes d'IA agentiques ressemblant plus à des agents intelligents qu'à des chatbots. GPT-5 peut générer des textes, du code informatique, des images et des applications

logicielles complètes, tout en naviguant dans le calendrier de l'utilisateur ou créant des résumés de recherche.

Le système comprend un modèle rapide et à haut débit, un modèle de raisonnement plus approfondi et un routeur temps réel décidant du modèle à utiliser selon le type de conversation. L'utilisateur peut choisir entre une meilleure réponse (plus approfondie avec délai d'attente) ou une réponse plus rapide et moins complète, disposant d'une fenêtre de contexte plus grande permettant de traiter des documents volumineux sans perte de cohérence.

VII.4 Réalisation pratique

La tâche consistait à utiliser l'intelligence artificielle pour générer une vidéo dans laquelle le chef de groupe dispense aux étudiants le premier chapitre de l'unité d'enseignement. GPT-5, de par sa capacité à générer textes, code et images, a permis la réalisation d'un script utilisé dans HeyGen pour générer la vidéo, grâce aux instructions, scénarios décrits et contenu du premier chapitre du cours. Il a également créé un prompt précis et concis permettant à HeyGen de générer une vidéo réaliste.

HeyGen offre plusieurs fonctionnalités avantageuses. L'avatar IA transforme une simple photo en avatar parlant ultra-réaliste (humains, animaux, créatures fantastiques), créant une identité visuelle unique renforçant l'image de marque professionnelle. La voix synthétique avancée et le clonage vocal proposent plus de trois cents voix dans plus de cent soixante-quinze langues, avec ajustement de l'accent, l'intonation et la vitesse d'élocution.

Le clonage vocal reproduit fidèlement une voix à partir d'un enregistrement audio, créant un discours impossible à distinguer de la parole humaine authentique. La traduction et localisation multilingue permettent la production vidéo dans plus de quarante langues avec synchronisation labiale parfaite. L'écosystème créatif et les intégrations permettent d'automatiser complètement la chaîne de production vidéo tout en maintenant une qualité broadcast.

Le processus de création comprend la sélection d'un template parmi plus de trois cents modèles disponibles, le choix d'un avatar personnalisant la vidéo, la rédaction du script avec sélection de la voix, du ton et de la vitesse d'élocution, l'ajout de ressources personnelles (vidéos, photos), et la soumission générant la vidéo en quelques minutes.

VII.5 Conclusion

Ce travail a démontré le potentiel de l'intelligence artificielle générative dans la création de contenus audiovisuels réalistes, en associant GPT pour la production du script et HeyGen pour la génération de la vidéo. Cette démarche a mis en évidence la complémentarité entre le traitement du langage naturel et la synthèse d'images, tout en offrant un aperçu des possibilités pédagogiques et communicationnelles offertes par les deepfakes.

Toutefois, cette expérience souligne l'importance de considérer les limites techniques, les risques d'abus et les enjeux éthiques liés à l'utilisation de telles technologies. À travers cette réalisation, le groupe a non seulement exploré une nouvelle approche de production multimédia, mais aussi ouvert la voie à une réflexion plus large sur l'avenir des outils d'IA générative et leur intégration responsable dans la société, démontrant l'impératif d'un usage encadré et éthique de ces technologies puissantes.

VIII Protocoles Post-Quantiques pour le CLO

VIII.1 Introduction et problématique

Ce document présente une synthèse détaillée de trois contributions majeures à la cryptographie post-quantique appliquée au CLO (Cryptography Legal Opposability) et à l'investigation numérique moderne. L'avènement des ordinateurs quantiques impose de repenser les preuves numériques pour garantir la non-répudiation (impossibilité pour un acteur de nier ses actions), la confidentialité (protection des données sensibles) et l'opposabilité juridique (valeur probante devant un tribunal).

Le CLO formalise ces exigences, et les protocoles post-quantiques comme ZK-NR et AIIP permettent de construire des preuves juridiquement fiables et sécurisées. Cette synthèse inclut des schémas, tableaux et exemples d'application pour enrichir la compréhension et montrer l'impact concret de ces approches sur la sécurisation des preuves numériques et l'opposabilité légale.

VIII.2 ZK-NR : Design et architecture multicouche

Le protocole ZK-NR vise à produire des preuves vérifiables et non-répudiables, assurer l'opposabilité légale des preuves, préserver la confidentialité des informations sensibles et garantir la résistance post-quantique face aux ordinateurs quantiques. Il s'appuie sur trois couches dialectiques formant une architecture stratifiée.

La couche Iron (Fer) assure la fiabilité via l'intégrité de base, la journalisation et les preuves minimales. La couche Gold (Or) garantit la confidentialité en fournissant des preuves contextuelles détaillées mais confidentielles. La couche Clay (Argile) assume l'opposabilité par l'enregistrement complet sur ledger pour auditabilité et traçabilité.

Les composants principaux incluent les Merkle Commitments assurant un engagement immuable des données, les STARK Proofs permettant la validation zero-knowledge post-quantique, les signatures Threshold BLS distribuées renforçant la non-répudiation, et Dilithium fournissant l'authentification post-quantique pour sécuriser la preuve. Le flux de données traverse séquentiellement la couche Iron, puis Gold, pour aboutir à l'enregistrement dans la couche Clay.

Les avantages incluent la non-répudiation absolue, la préservation de la confidentialité (privacy-preserving) et la sécurité post-quantique. Cependant, plusieurs défis persistent : la complexité technique nécessite la formation des magistrats et enquêteurs, l'interopérabilité requiert l'adoption de standards internationaux pour la validité juridique, et les performances souffrent d'un overhead computationnel important lié aux preuves zero-knowledge et signatures post-quantiques.

VIII.3 CRO Trilemma et UC-Security

Le Trilemme CRO établit l'incompatibilité fondamentale entre trois propriétés : la Confidentialité, la Fiabilité et l'Opposabilité juridique. Cette formalisation mathématique démontre qu'il est impossible de maximiser simultanément ces trois dimensions, imposant des compromis mesurés par l'indice gamma CRO qui doit rester supérieur ou égal à 0,4 plus une fonction négligeable du paramètre de sécurité lambda.

L'architecture Q2CSI (Quantum-to-Classical Security Infrastructure) propose une solution détaillée à ce trilemme via trois couches spécialisées. La couche Clay assure l'ancrage institutionnel et l'opposabilité juridique. La couche Gold préserve l'entropie sémantique et la confidentialité des données sensibles. La couche Iron garantit l'intégrité temporelle et la journalisation rigoureuse des événements.

La sécurité UC (Universal Composability) modélise chaque couche comme une fonctionnalité idéale avec sémantique d'effacement, permettant la preuve de composabilité universelle post-quantique. Cette approche atteint un indice gamma CRO inférieur à 0,4 plus une fonction négligeable, démontrant une résistance robuste contre les adversaires adaptatifs contextuels tout en minimisant la violation du trilemme.

VIII.4 AIIP : Fondement post-quantique

Le problème AIIP (Affine Iterated Inversion Problem) constitue un nouveau problème de dureté post-quantique fondé sur l'inversion affine itérée. Étant donné un polynôme f dans un corps fini de degré d supérieur ou égal à deux, un paramètre d'itération n, et un objectif y, le problème consiste à trouver x tel que l'application n fois itérée de f sur x égale y.

La dureté post-quantique d'AIIP repose sur sa connexion au logarithme discret sur courbes hyperelliptiques de genre exponentiellement grand. Il existe une réduction en temps polynomial à des systèmes multivariés quadratiques (MQ), reconnus NP-difficiles. Le cas quadratique particulier où f(x) égale x au carré plus alpha produit un système MQ heuristiquement indiscernable d'un système aléatoire.

Les applications concrètes incluent les signatures numériques post-quantiques vérifiables et non-répudiables, le chiffrement à clé publique résistant aux attaques quantiques, et un complément essentiel aux architectures ZK-NR pour le CLO. La comparaison avec ZK-NR montre des différences notables : ZK-NR utilise STARK, Dilithium et BLS pour la résistance post-quantique, tandis qu'AIIP s'appuie sur les problèmes MQ et courbes hyperelliptiques. La confidentialité est élevée (zero-knowledge) pour ZK-NR mais moyenne (fonction des preuves) pour AIIP. Les deux garantissent la non-répudiation via différents mécanismes mathématiques.

VIII.5 Scénarios d'utilisation

Dans l'investigation judiciaire numérique, ces protocoles permettent la création de preuves juridiquement opposables sans divulguer les données sensibles. La vérification par un tribunal s'effectue via la couche Clay, tandis que l'auditabilité postérieure est assurée par le ledger immuable. Ce mécanisme garantit simultanément la protection des informations confidentielles et la validité juridique des éléments de preuve.

Pour la signature et transmission de documents sensibles, la signature via AIIP ou Dilithium garantit la non-répudiation, empêchant toute contestation ultérieure de l'authenticité. La transmission sécurisée et vérifiable grâce à ZK-NR assure que les documents parviennent intacts à leurs destinataires tout en maintenant leur confidentialité contre les interceptions.

VIII.6 Synthèse comparative

Le protocole ZK-NR fournit des attestations zero-knowledge non-répudiables et juridiquement explicables, s'appuyant sur STARK Proofs, Threshold BLS, Dilithium et Merkle Commitments. Son impact sur le CLO et l'investigation numérique permet la création de preuves vérifiables, confidentielles et opposables juridiquement, renforçant la non-répudiation et la traçabilité des actions numériques.

Le CRO Trilemma avec l'architecture Q2CSI formalise les compromis entre Confidentialité, Fiabilité et Opposabilité juridique via les indices gamma CRO et l'architecture multicouche Clay-Gold-Iron. Il aide à gérer les trade-offs dans les preuves numériques, assure la sécurité composable et post-quantique, et facilite la vérification judiciaire tout en préservant la confidentialité.

Le problème AIIP fournit une primitive post-quantique pour signatures numériques et chiffrement, reposant sur l'Affine Iterated Inversion Problem avec réduction aux systèmes MQ NP-difficiles et connexion aux courbes hyperelliptiques. Il offre une base mathématique pour concevoir des signatures et chiffrement post-quantiques, soutenant la non-répudiation et l'opposabilité juridique dans les systèmes numériques.

VIII.7 Conclusion

Les trois contributions combinées fournissent un cadre complet pour l'investigation numérique post-quantique et le CLO. Le protocole ZK-NR offre une architecture multicouche pour preuves légalement opposables. Le CRO Trilemma formalise les limites et trade-offs entre confidentialité, fiabilité et opposabilité. Le problème AIIP constitue une fondation cryptographique post-quantique pour signatures et chiffrement.

L'intégration de ces approches permet de construire des systèmes robustes, vérifiables et résilients aux menaces quantiques. Les scénarios d'usage démontrent l'applicabilité concrète des protocoles pour l'investigation numérique et la gestion sécurisée de données sensibles. Cette synthèse établit les bases théoriques et pratiques nécessaires pour l'évolution des systèmes de preuve numérique dans l'ère post-quantique, garantissant simultanément sécurité cryptographique et opposabilité juridique.