RÉPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
*****
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
*****
DÉPARTEMENT DE GÉNIE INFORMATIQUE
*****

REPUBLIC OF CAMEROON
Peace – Work – Fatherland
*****
MINISTRY OF HIGHER EDUCATION
*****
UNIVERSITY OF YAOUNDE I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
COMPUTER ENGINEERING DEPARTMENT
*****

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

RESUMES DES EXPOSES

Rédigé par
NZOUCK TOUMPE ERIC - OLIVIER
Matricule : ***22P060***

Sous la supervision de
Thierry MINKA, Eng

Année académique 2025/2026

EXPOSÉ 1 : POINTS SUR LES ALGORITHMES DE RECONNAISSANCE FACIALE

La reconnaissance faciale constitue une technologie sophistiquée d'intelligence artificielle, permettant d'identifier ou de vérifier l'identité d'un individu à partir de ses traits faciaux. Elle repose sur l'analyse de caractéristiques uniques telles que la distance inter-oculaire, la forme du nez, des lèvres ou le contour de la mâchoire. Cette technologie utilise des systèmes biométriques structurés autour de plusieurs étapes essentielles :

1. L'enrôlement : les données faciales sont capturées, traitées et stockées de manière sécurisée dans une base de données.
2. L'identification : elle consiste à comparer un individu à l'ensemble des profils existants dans la base (recherche 1-N).
3. La vérification : elle confirme ou infirme l'identité déclarée d'une personne (recherche 1-1).

Les algorithmes employés varient des techniques classiques, globales ou locales, telles que PCA, LDA, EBGM ou HMM, aux approches hybrides et aux modèles de deep learning récents. Des détecteurs et descripteurs de points clés comme SIFT, HOG ou SURF renforcent la robustesse face aux variations de lumière, de pose ou d'expression faciale.

La reconnaissance faciale est devenue un outil stratégique dans le domaine de la cybersécurité et de l'investigation numérique. Elle permet de traiter efficacement de vastes volumes de données visuelles issues de vidéosurveillance, de réseaux sociaux ou d'appareils saisis, facilitant l'identification des suspects et la reconstitution des événements.

Cependant, cette technologie présente certaines limites importantes :

- Le biais algorithmique, pouvant générer des discriminations involontaires ;

- Les risques de falsification ou d'usurpation via deepfakes, vulnérabilités techniques ou atteintes à la vie privée ;
- Les contestations juridiques liées à la collecte et à l'utilisation des données biométriques.

Pour garantir son efficacité et sa légalité, la reconnaissance faciale nécessite une supervision humaine, une documentation détaillée des processus, des audits réguliers, la protection stricte des données et un cadre juridique clair. Lorsqu'elle est correctement encadrée, elle offre un atout majeur, combinant rapidité, précision et traçabilité, tout en respectant les droits fondamentaux, ce qui est particulièrement crucial dans un contexte comme le Cameroun, où l'éthique et la régulation sont essentielles pour la légitimité des enquêtes numériques.

EXPOSÉ 2 : SIMULATION D'UNE SÉRIE DE MESSAGES SUR WHATSAPP ENTRE UN HOMME ET SA MAÎTRESSE

L'objectif de cet exposé était de démontrer la facilité avec laquelle de fausses preuves numériques peuvent être créées et d'analyser les conséquences de ces manipulations sur la fiabilité des éléments utilisés lors d'enquêtes judiciaires ou disciplinaires.

Pour mener cette simulation, deux outils principaux ont été utilisés :

1. Chatsmock : permet de générer de fausses conversations WhatsApp en personnalisant les noms, messages, horaires et statuts.
2. Adobe Photoshop : utilisé pour retoucher les captures d'écran et rendre les échanges plus réalistes.

L'étude a mis en évidence certaines limites de Chatsmock, notamment un manque de réalisme sur certains détails graphiques et la possibilité pour un expert de détecter la falsification grâce aux métadonnées. Une comparaison avec d'autres outils tels que FakeChat, WhatsFake et Photoshop a montré que certains offrent davantage d'options, mais nécessitent un niveau technique plus élevé.

Les risques liés à l'usage de ces outils sont multiples :

- Perte de confiance dans les preuves numériques ;
- Possibilité de manipulations judiciaires ;
- Complexification du travail des enquêteurs.

Plusieurs recommandations ont été formulées :

- Vérifier systématiquement les métadonnées et l'authenticité des preuves ;
- Former et sensibiliser les acteurs du domaine judiciaire ;
- Privilégier les données brutes plutôt que les simples captures d'écran ;
- Renforcer le cadre légal encadrant l'usage des preuves numériques.

En résumé, la falsification de preuves numériques est simple mais potentiellement dangereuse, soulignant la nécessité de méthodes d'analyse robustes pour préserver l'intégrité et la fiabilité des enquêtes numériques.

EXPOSÉ 3 : LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

Cet exposé portait sur l'analyse comparative de trois outils académiques largement utilisés pour la rédaction de mémoires : Overleaf, Microsoft Word et Zotero. L'objectif était d'identifier leurs avantages, limites et combinaisons optimales pour aider les étudiants à choisir les solutions les plus adaptées à leurs besoins.

1. **Overleaf** : Éditeur LaTeX en ligne, Overleaf facilite la rédaction scientifique et collaborative. Ses points forts incluent une typographie professionnelle, la gestion automatisée des références croisées et la collaboration en temps réel. Ses limites concernent une courbe d'apprentissage élevée, l'édition hors ligne restreinte et une complexité pour les débutants. Des alternatives comme LyX, TeXmaker ou Authorea peuvent être envisagées pour divers

besoins académiques. Overleaf reste idéal pour les travaux scientifiques nécessitant rigueur et précision.

2. **Microsoft Word** : Ce traitement de texte universel est le logiciel le plus répandu dans le milieu académique, grâce à sa simplicité et sa compatibilité universelle. Ses points forts incluent la gestion des styles hiérarchiques, la génération automatique de tables et sommaires, le suivi des modifications et la compatibilité avec de nombreux formats. Ses limites concernent la gestion bibliographique limitée, des risques d'instabilité sur les documents longs et une structuration parfois incohérente si les styles sont mal appliqués. Word convient particulièrement aux étudiants recherchant simplicité et rapidité d'utilisation.

3. **Zotero** : Logiciel gratuit et open-source dédié à la gestion bibliographique, Zotero permet de collecter automatiquement les références depuis des bases de données, d'organiser les sources et de générer des citations et bibliographies selon différents styles (APA, MLA, Chicago, etc.). Il s'intègre facilement à Word et Overleaf. Des alternatives incluent Mendeley, EndNote ou Citavi. Zotero est un outil complet pour gérer efficacement les sources académiques.

Il convient de rappeler que, malgré la puissance de ces outils, la réussite d'un mémoire repose avant tout sur la profondeur de réflexion et la maîtrise du sujet traité.

EXPOSÉ 4 : CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK

Dans le cadre de cette étude, un faux profil TikTok a été créé sur la thématique de la cybersécurité afin d'analyser les comportements et réactions des utilisateurs dans un contexte pédagogique et éthique.

La démarche méthodologique a suivi plusieurs étapes :

1. Création du profil avec une adresse temporaire ;

2. Choix d'une niche pertinente permettant de combiner sensibilisation et apprentissage technique ;
3. Développement d'une stratégie de contenu mêlant informations éducatives, messages interactifs, visuels attractifs et ton léger pour favoriser l'engagement.

Les thématiques abordées incluaient la sécurité des mots de passe, la protection des données personnelles, le phishing et les risques liés aux réseaux Wi-Fi publics. Le suivi des interactions a été réalisé à l'aide des statistiques internes de TikTok, de captures d'écran et d'outils complémentaires tels que ChatGPT pour la rédaction et Canva pour les visuels.

L'analyse a montré l'efficacité de cette stratégie pour capter l'attention et susciter l'intérêt des utilisateurs, tout en soulignant les limites éthiques liées à la création de faux profils, nécessitant un encadrement strict pour éviter toute manipulation ou malentendu.

Les recommandations principales comprenaient :

- Renforcer l'éducation à la cybersécurité dès le secondaire ;
- Intégrer des exercices pratiques ;
- Favoriser la collaboration interdisciplinaire pour sensibiliser efficacement les utilisateurs tout en respectant les principes de sécurité numérique.

Cette expérience illustre que l'investigation numérique peut être interactive, utile et impactante pour l'apprentissage, à condition de respecter un cadre éthique strict.

EXPOSÉ 5 : DEEPFAKE VOCAL

Cet exposé portait sur les deepfakes audio, et plus spécifiquement le clonage vocal, qui consiste à reproduire la voix d'une personne via intelligence artificielle et deep learning.

L'évolution de cette technologie a été rappelée, depuis les premières synthèses vocales des années 1930 jusqu'aux outils modernes comme

WaveNet, Tacotron ou Real-Time-Voice-Cloning, rendant le clonage vocal réaliste et accessible.

Les applications légitimes incluent :

- L'accessibilité pour les personnes souffrant de troubles de la parole ;
- Le doublage multilingue ;
- L'amélioration des assistants vocaux.

Cependant, les risques restent importants : usurpation d'identité, fraude financière ou manipulation de l'opinion publique. Le cas pratique de MINIMAX audio a illustré comment des voix peuvent être clonées à partir d'échantillons réels pour produire des messages jamais prononcés par le locuteur.

Les enjeux pour l'investigation numérique incluent :

- La compromission de la confidentialité et de la fiabilité des preuves audio ;
- La nécessité de maîtriser les modèles techniques pour détecter les falsifications.

Les mesures préventives recommandées comprennent :

- La détection technologique des deepfakes ;
- La sensibilisation des utilisateurs ;
- Le renforcement du cadre légal ;
- L'authentification multi-facteurs ;
- La promotion d'une éthique de l'IA.

Seule une approche combinant technologie, réglementation et gouvernance permet de limiter les abus tout en exploitant positivement ces outils.

EXPOSÉ 6 : L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

L'investigation numérique s'impose aujourd'hui comme un outil central pour la police judiciaire, notamment dans un contexte où la criminalité contemporaine exploite massivement les technologies numériques. Elle permet de collecter, analyser et préserver des preuves provenant d'ordinateurs, de téléphones, de réseaux ou de tout autre support électronique, offrant un accès à des informations souvent invisibles dans le monde physique, telles que des fichiers effacés, des historiques de navigation, des métadonnées ou des communications supprimées.

Cette discipline facilite la lutte contre la cybercriminalité et contribue à résoudre des affaires de piratage, de fraude en ligne ou d'usurpation d'identité. Elle permet également d'identifier et de suivre les auteurs grâce à l'analyse d'adresses IP, de journaux système et de données de géolocalisation. L'investigation numérique offre la possibilité de reconstituer précisément la chronologie des événements, de suivre les flux financiers, de relier des suspects et de produire des preuves recevables en justice, renforçant ainsi l'efficacité des enquêtes traditionnelles.

Ses domaines d'application sont variés :

- Lutte contre la cybercriminalité et la criminalité transfrontalière ;
- Prévention et investigation du terrorisme ;
- Enquêtes sur les crimes économiques et financiers ;
- Criminalité organisée ;
- Protection de l'enfance ;
- Coopération avec des organisations internationales pour traquer des réseaux criminels à l'échelle mondiale.

Néanmoins, l'investigation numérique au Cameroun fait face à des défis considérables : explosion et complexité des données, évolution rapide des technologies, pénurie d'experts qualifiés, contraintes matérielles

et financières, ainsi que limites juridiques sur l'admissibilité et l'intégrité des preuves.

Malgré ces obstacles, elle demeure un levier stratégique pour la sécurité nationale et la souveraineté judiciaire, permettant de prévenir de nouvelles menaces comme les deepfakes ou l'usage malveillant de l'intelligence artificielle, tout en garantissant que la justice repose sur des preuves fiables, traçables et opposables légalement.

EXPOSÉ 7 : PRÉSENTATION DÉTAILLÉE DU PROTOCOLE ZK-NR

Le protocole ZK-NR (Zero-Knowledge Non-Repudiation) représente une avancée majeure dans le domaine de l'investigation numérique, en alliant sécurité cryptographique, confidentialité et opposabilité juridique. Conçu pour répondre aux besoins croissants des enquêteurs et magistrats, il permet de garantir l'intégrité des preuves numériques, d'assurer la traçabilité complète des actes et de prouver l'origine des données sans divulguer leur contenu sensible, grâce aux preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs).

ZK-NR est particulièrement adapté aux environnements réglementés, tels que la finance, l'e-gouvernement ou la cybersécurité, où les exigences légales sur la recevabilité des preuves numériques sont strictes. En utilisant des primitives post-quantiques comme STARKs, Dilithium ou SPHINCS+, il anticipe les menaces liées à l'informatique quantique et protège les preuves contre toute falsification ou usurpation.

Intégré au cadre CLO (Cryptographic Legal Opposability), ZK-NR formalise la valeur juridique des preuves numériques, assurant leur auditabilité et leur explicabilité institutionnelle. Dans la pratique, ce protocole permet de :

- Créer des attestations invisibles mais vérifiables ;
- Sceller cryptographiquement la chaîne de possession (chain of custody) ;

- Produire des preuves opposables devant un tribunal tout en préservant la confidentialité des informations sensibles.

Son efficacité se manifeste dans des cas concrets tels que l'analyse de transactions frauduleuses dans des affaires de cyberfraude bancaire au Cameroun, la détection d'escroqueries BEC, le démantèlement de réseaux de SIMBOX, et des opérations internationales comme l'infiltration du système EncroChat en Europe.

ZK-NR et CLO dépassent les méthodes traditionnelles basées sur le hashing ou les signatures électroniques classiques, en combinant sécurité technique avancée, conformité juridique et robustesse post-quantique. Cette convergence crypto-légale transforme l'investigation numérique en un processus intégral, où la cryptographie garantit la fiabilité, la vérifiabilité et l'opposabilité juridique des preuves.

EXPOSÉ 8 : LES 10 CAS AFRICAINS LES PLUS IMPORTANTS DU HACKING DURANT LES 10 DERNIÈRES ANNÉES

Le continent africain, bien que connaissant une croissance numérique rapide, a également vu émerger une augmentation significative des cyberattaques. Selon des rapports, notamment d'Interpol, le continent subit désormais plus de 3 000 attaques par semaine et par organisation.

L'étude a présenté dix incidents majeurs, tels que :

- L'attaque par ransomware contre Transnet en Afrique du Sud (2021) ;
- Le piratage de la CNSS au Maroc (2025) ;
- L'attaque contre ENEO au Cameroun (2024) ;
- La fraude Mobile Money au Nigeria (2018).

Ces exemples démontrent que tous les secteurs — public, privé, financier, sanitaire et industriel — sont exposés, avec des pertes financières souvent importantes et des fuites massives de données sensibles.

La plupart des pays africains souffrent encore d'un manque d'experts qualifiés, de cadres juridiques solides et de moyens techniques adaptés pour contrer ces menaces. Les recommandations incluent :

- Former davantage de spécialistes en cybersécurité ;
- Créer des centres de réponse régionaux (CERT) ;
- Renforcer la coopération entre États ;
- Encourager l'hébergement local des données pour renforcer la souveraineté numérique africaine.

Il est clair que la cybersécurité devient un élément indispensable pour le développement durable et sécurisé du continent.

EXPOSÉ 9 : DEEPFAKE : RÉALISATION D'UNE VIDÉO À L'AIDE DE L'IA

Cet exposé a présenté une vidéo pédagogique utilisant les intelligences artificielles GPT-5 et HeyGen AI pour illustrer un chapitre d'un cours d'investigation numérique.

Le projet consistait à créer un deepfake vidéo, dans lequel un avatar animé dispense le cours comme le ferait un enseignant humain. Le processus a été réalisé en deux étapes :

1. Rédaction du script via GPT-5, structurant le contenu et les instructions de scénarisation ;
2. Génération de la vidéo avec HeyGen AI, animant l'avatar et produisant une voix synthétique naturelle et multilingue.

Cette démarche montre comment les IA peuvent rendre l'apprentissage plus interactif et immersif, tout en facilitant la production de contenus audiovisuels de qualité, sans compétences techniques avancées.

L'exposé a également abordé les enjeux éthiques et techniques des deepfakes, notamment :

- Les risques de manipulation ;

- La protection des droits à l'image ;
- La nécessité d'une utilisation responsable et encadrée.

En combinant traitement du langage naturel et synthèse vidéo, cette expérience illustre le potentiel des intelligences artificielles génératives pour transformer la pédagogie et la communication numérique, tout en soulignant l'importance d'une intégration sécurisée et éthique de ces technologies.

CONCLUSION GÉNÉRALE

L'ensemble des travaux présentés met en lumière l'évolution rapide des technologies numériques et cryptographiques, ainsi que leur impact significatif sur l'investigation et la pédagogie modernes. Du protocole ZK-NR, garantissant sécurité post-quantique, non-répudiation et opposabilité juridique, à l'usage des intelligences artificielles génératives pour produire des contenus pédagogiques immersifs, il apparaît que l'innovation technologique et les exigences institutionnelles sont désormais indissociables.

La protection, l'authenticité et la fiabilité des données numériques ne sont plus de simples enjeux techniques, mais des éléments essentiels pour assurer la confiance, la traçabilité et la recevabilité légale dans des contextes variés : enquêtes judiciaires, cybersécurité ou éducation.

Enfin, ces recherches soulignent l'importance de combiner performance technologique et responsabilité éthique : l'essor des deepfakes, des preuves cryptographiques post-quantiques et des IA génératives doit s'accompagner de cadres réglementaires solides et de pratiques encadrées, afin que l'innovation serve la société tout en protégeant la sécurité, la confidentialité et l'intégrité des informations.