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

RESUME DES EXPOSES

N°	MLE	NOMS ET PRÉNOMS	NOTE
1	22P064	MENGUE BISSA MARGUERITE	

Sous la supervision de : M.MINKA Thierry

ANNÉE ACADÉMIQUE 2025 – 2026

EXPOSE 1:POINTS SUR LES ALGORITHMES DE RECONNAISSANCE FACIALE

La reconnaissance faciale est une technologie avancée d'intelligence artificielle permettant d'identifier ou de vérifier l'identité d'une personne à partir de ses traits du visage, en analysant des caractéristiques uniques telles que la distance entre les yeux, la forme du nez, des lèvres ou du contour de la mâchoire. Elle s'appuie sur des **systèmes biométriques** structurés autour de plusieurs étapes :

- L'enrôlement, où les données faciales sont capturées et stockées dans une base sécurisée ;
- L'identification, qui permet de comparer un individu à l'ensemble des profils existants (recherche 1-N)
- La vérification, qui confirme ou infirme une identité déclarée (recherche 1-1).

Les algorithmes utilisés varient des méthodes classiques globales ou locales (PCA, LDA, EBGM, HMM) aux approches hybrides et aux techniques modernes de deep learning, tandis que des détecteurs et descripteurs de points d'intérêt comme SIFT, HOG ou SURF permettent d'assurer la robustesse face aux variations de lumière, de pose ou d'expression. Cette technologie est devenue un outil stratégique dans l'investigation numérique et la cybersécurité, car elle permet de traiter rapidement de vastes volumes de données visuelles issues de vidéo-surveillances, de réseaux sociaux ou de dispositifs saisis, facilitant ainsi l'identification de suspects et la reconstitution d'événements. Cependant, son usage présente des limites importantes :

- Le biais algorithmique pouvant entraîner des discriminations;
- Les risques d'usurpation ou de manipulation via deepfakes, vulnérabilités techniques, atteintes à la vie privée et contestations juridiques liées à la légalité des données biométriques collectées.

Pour être efficace et légalement recevable, la reconnaissance faciale nécessite donc une supervision humaine, une documentation complète

des processus, des audits réguliers, la protection stricte des données et un cadre juridique clair garantissant proportionnalité et finalité de l'usage.Lorsqu'elle est correctement encadrée, cette technologie représente un atout majeur permettant de combiner rapidité, précision et traçabilité tout en conciliant innovation technologique et respect des droits fondamentaux, particulièrement dans des contextes sensibles comme le Cameroun, où la régulation et l'éthique jouent un rôle central dans la légitimité des enquêtes numériques.

EXPOSE 2:SIMULATION D'UNE SERIE DE MESSAGES SUR WHATSAPP ENTRE UNE HOMME ET SA MAITRESSE

L'objectif était de montrer qu'il est facile de créer de fausses preuves numériques et d'analyser les conséquences de ces manipulations sur la fiabilité des éléments utilisés lors d'enquêtes judiciaires ou disciplinaires.

Pour réaliser cette simulation, deux outils ont été utilisés :

- Chatsmock, qui permet de générer de fausses conversations WhatsApp en personnalisant les noms, les messages, les heures et les statuts ;
- Adobe Photoshop, employé pour retoucher les captures d'écran et rendre les échanges plus réalistes.

Le travail a également mis en évidence les limites de Chatsmock, notamment son manque de réalisme sur certains détails graphiques et la possibilité pour un expert de repérer la falsification à travers les métadonnées. Une comparaison avec d'autres outils comme FakeChat, WhatsFake et Photoshop a permis de montrer que certains offrent plus d'options, mais demandent plus de compétences techniques.L'étude a souligné les risques liés à l'utilisation de ces outils : perte de confiance dans les preuves numériques, risque de manipulation judiciaire et complexité accrue du travail des enquêteurs.Plusieurs recommandations ont été proposées :

- Vérifier 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 les preuves numériques.

Nous pouvons donc dire que la falsification de preuves numériques est simple mais dangereuse, et qu'il est essentiel de renforcer les méthodes d'analyse pour garantir la fiabilité et l'intégrité des preuves dans les enquêtes numériques.

EXPOSE 3:LES TROIS MEILLEURS LOGICIELS DE REDACTION DE MEMOIRE

Le travail qui avait été présenté portait sur l'analyse comparative de trois outils académiques utilisés pour la rédaction des mémoires : Overleaf, Microsoft Word et Zotero. L'objectif principal était de déterminer les avantages, limites et combinaisons optimales de ces logiciels afin d'aider les étudiants à choisir les outils les plus adaptés à leurs besoins.

1.Overleaf

L'excellence académique par LaTeX est un éditeur LaTeX en ligne, créé pour faciliter la rédaction scientifique et collaborative.Il se distingue par une qualité typographique professionnelle,une gestion automatisée des références croisées,et une collaboration en temps réel,une courbe d'apprentissage élevée,une édition hors ligne restreinte,et un usage parfois complexe pour les débutants.Des alternatives comme LyX, TeXmaker ou Authorea ont également été évoquées.Overleaf est donc idéal pour les travaux scientifiques exigeant rigueur et précision.

2.Microsoft Word

Le traitement de texte universel;il reste le logiciel le plus utilisé dans le monde académique, grâce à sa simplicité et son accessibilité.Il se dis-

tingue par la gestion des styles hiérarchiques,la création automatique de tables et sommaires,le suivi des modifications et la compatibilité universelle.Ses faiblesses concernent une gestion bibliographique limitée,des risques d'instabilité sur les longs documents,et une structuration parfois incohérente si les styles ne sont pas bien appliqués.Word convient surtout aux étudiants qui recherchent la simplicité et la rapidité d'utilisation.

3.Zotero

Le spécialiste de la bibliographie,est un logiciel gratuit et open-source dédié à la gestion des références bibliographiques.Il permet de collecter automatiquement les références depuis les bases de données,organiser les sources et générer automatiquement les citations et la bibliographie selon différents styles (APA, MLA, Chicago, etc.).Il s'intègre facilement à Word et à Overleaf.Parmi ses alternatives, on retrouve Mendeley, EndNote et Citavi.Zotero est l'outil le plus complet et le plus accessible pour gérer efficacement les sources académiques.

Il a été rappelé qu'aussi puissants soient-ils, ces outils ne remplacent pas la qualité du contenu : la réussite d'un mémoire repose avant tout sur la profondeur de la réflexion et la maîtrise du sujet.

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

Dans le cadre de cette investigation numérique, nous avons créé un faux profil TikTok autour de la thématique de la cybersécurité afin d'analyser les comportements et les réactions des utilisateurs dans un contexte pédagogique et éthique. La démarche méthodologique a débuté par la création du profil avec une adresse temporaire, suivie du choix d'une niche pertinente et sensible, permettant d'allier sensibilisation et apprentissage technique. La stratégie de contenu adoptée combinait informations éducatives, messages interactifs, visuels attractifs et un ton léger pour favoriser l'engagement, en abordant des

sujets comme la sécurité des mots de passe, la protection des données personnelles, le phishing ou les risques liés au Wi-Fi public. Le suivi des interactions a été assuré grâce aux statistiques internes de TikTok, aux captures d'écran et à des outils complémentaires comme ChatGPT pour la rédaction de contenus et Canva pour les visuels. L'analyse a montré que cette stratégie était pertinente pour capter l'attention et susciter l'intérêt des utilisateurs, tout en soulignant les limites éthiques liées à la création de faux profils, qui nécessitent un encadrement strict pour éviter toute manipulation ou malentendu. Ce projet a permis de mesurer l'efficacité des messages de prévention sur les réseaux sociaux, d'illustrer l'importance d'une approche responsable et réfléchie, et de proposer des recommandations telles que le renforcement de l'éducation à la cybersécurité dès le secondaire, l'intégration d'exercices pratiques et la promotion d'une collaboration interdisciplinaire pour sensibiliser les utilisateurs tout en respectant les principes de sécurité numérique. En somme, cette expérience démontre que l'investigation numérique peut être interactive, impactante et utile pour l'apprentissage, tout en mettant en lumière la nécessité d'un usage éthique et encadré des outils digitaux.

EXPOSE 5:Deepfake VOCAL

Le travail présenté portait sur le phénomène des deepfakes audios, et plus particulièrement le deepfake vocal, qui consiste à imiter la voix d'une personne grâce à l'intelligence artificielle et au deep learning.Il nous a d'abord été rappelé l'évolution de cette technologie, depuis les premières synthèses vocales des années 1930 jusqu'aux outils modernes comme WaveNet, Tacotron ou Real-Time-Voice-Cloning, qui ont rendu le clonage vocal accessible et réaliste. Ces technologies pouvaient être utilisées à des fins légitimes, comme l'accessibilité pour les personnes souffrant de troubles de la parole, le doublage multilingue ou l'amélioration des assistants vocaux, mais qu'elles représentaient également des risques importants pour la cybersécurité, l'éthique et la justice. À travers le cas pratique de MINIMAX audio, il a été illustré

comment une voix pouvait être clonée à partir d'échantillons réels pour générer des messages jamais prononcés par le locuteur, soulignant les usages malveillants possibles tels que l'usurpation d'identité, la fraude financière ou la manipulation de l'opinion publique. Les enjeux pour l'investigation numérique ont été analysé, en montrant que ces deepfakes compromettaient la confidentialité, la fiabilité et l'opposabilité des preuves audio, et qu'ils nécessitaient une compréhension approfondie des modèles techniques pour être détectés. Des contre-mesures et moyens de prévention, incluant la détection technologique, la sensibilisation des utilisateurs, le renforcement du cadre légal, la sécurisation par authentification multi-facteur et la promotion d'une éthique de l'IA, concluant que seule une approche combinant technologie, réglementation et gouvernance permettrait de limiter les abus tout en tirant parti des applications positives de ces outils.

EXPOSE 6:L'UTILITE DE L'INVESTIGATION NUMERIQUE DANS LA POLICE JUDICIAIRE

L'investigation numérique s'est imposée comme un outil fondamental pour la police judiciaire, en particulier dans un contexte où la criminalité moderne 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 fichiers effacés, historiques de navigation, métadonnées ou communications supprimées en facilitant la lutte contre la cybercriminalité, permettant de résoudre des affaires de piratage, de fraude en ligne ou d'usurpation d'identité, et contribue à l'identification et au traçage des auteurs par l'analyse d'adresses IP, de journaux systèmes et de données de géolocalisation. Elle permet également de reconstituer avec précision la chronologie des événements, de suivre les flux financiers, de relier des suspects et de produire des preuves recevables en justice, renforçant l'efficacité des enquêtes traditionnelles. Ses domaines d'application sont nombreux :

lutte contre la cybercriminalité, criminalité transfrontalière et terrorisme, crimes économiques et financiers, criminalité organisée, protection de l'enfance, enquêtes judiciaires classiques, et coopération avec des organisations internationales pour traquer des réseaux criminels à l'échelle mondiale. Cependant, l'investigation numérique au Cameroun doit faire face à des défis considérables, notamment l'explosion et la complexité des données, l'évolution rapide des technologies, la pénurie d'experts qualifiés, les contraintes matérielles et financières, ainsi que les limites juridiques liées à l'admissibilité et à l'intégrité des preuves. Malgré ces obstacles, elle constitue un atout stratégique pour renforcer la sécurité nationale et la souveraineté judiciaire, en permettant aux forces de l'ordre de suivre l'évolution de la criminalité, de prévenir de nouvelles menaces telles que les deepfakes ou l'utilisation malveillante de l'intelligence artificielle, et de garantir que la justice repose sur des preuves fiables et traçables. L'investigation numérique n'est donc plus une option mais une nécessité pour faire face aux défis de la criminalité et sécuriser l'avenir numérique du pays.

EXPOSE 7:PRESENTATION DETAILLEE DU PROTOCOLE ZK-NR

Le protocole ZK-NR (Zero-Knowledge Non-Repudiation) représente une avancée majeure dans l'investigation numérique en conciliant 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 de manière irréfutable l'origine des données sans en révéler le contenu sensible, grâce aux preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs). Cette approche est particulièrement adaptée 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 s'appuyant sur des primitives post-quantiques comme STARKs, Dilithium ou SPHINCS+, ZK-NR anticipe les menaces liées

aux ordinateurs quantiques et garantit la résilience des preuves contre toute falsification ou usurpation. Le protocole est intégré dans le cadre CLO (Cryptographic Legal Opposability), qui formalise la valeur juridique des preuves numériques en assurant leur auditabilité et leur explicabilité institutionnelle. Dans la pratique, ZK-NR permet aux enquêteurs de créer des attestations invisibles mais vérifiables, de sceller cryptographiquement la chaîne de possession (chain of custody) et de produire des preuves opposables devant un tribunal, tout en préservant la confidentialité des informations sensibles. Son efficacité est illustrée par des cas concrets, tels que l'analyse des transactions frauduleuses dans des affaires de cyberfraude bancaire au Cameroun, la détection d'escroqueries BEC ou le démantèlement de réseaux de SIMBOX, ainsi que par des opérations internationales comme l'infiltration du système EncroChat en Europe. Dans le contexte de l'investigation numérique moderne, ZK-NR et CLO dépassent les méthodes classiques basées sur le simple hashing ou les signatures électroniques traditionnelles, en combinant sécurité technique avancée, conformité juridique et robustesse post-quantique. Cette convergence crypto-légale transforme la pratique forensique : l'investigation numérique ne se limite plus à la collecte de données, mais devient un processus intégral où la cryptographie garantit la fiabilité, la vérifiabilité et l'opposabilité juridique des preuves, établissant ainsi une nouvelle norme pour la preuve numérique dans un environnement toujours plus complexe et dématérialisé.

EXPOSE 8:LES 10 CAS AFRICAINS LES PLUS IMPORTANTS DU HACKING DURANT LES 10 DERNIERES ANNEES

L'Afrique a connu une croissance numérique rapide, mais cette transformation s'accompagnait d'une hausse inquiétante des cyberattaques. En s'appuyant sur des rapports comme celui d'Interpol, il a été souligné que le continent enregistrait désormais plus de 3 000 attaques par semaine et par organisation. L'étude présentait dix cas emblématiques, dont l'attaque de ransomware contre Transnet en Afrique du

Sud (2021), le piratage de la CNSS au Maroc (2025), l'attaque contre ENEO au Cameroun (2024), ou encore la fraude au Mobile Money au Nigeria (2018);ces exemples montraient que tous les secteurs public, privé, financier, sanitaire et industriel étaient touchés, avec des pertes financières parfois considérables et des fuites massives de données sensibles. La plupart des pays africains manquent encore d'experts qualifiés, de cadres juridiques solides et de moyens techniques adaptés pour répondre efficacement à ces menaces. Nonobstant, il a été recommandé de former davantage de spécialistes, de créer des centres de réponse régionaux (CERT), de renforcer la coopération entre États et de favoriser l'hébergement local des données pour atteindre une véritable souveraineté numérique africaine.

Nous pouvons dire que la cybersécurité doit être indispensable au développement durable et sécurisé du continent.

EXPOSE 9:DEEPFAKE: REALISATION D'UNE VIDEO A L'AIDE DE L'IA

Il nous été présenté une vidéo pédagogique exploitant les intelligences artificielles GPT-5 et HeyGen AI pour illustrer le premier chapitre d'un cours d'investigation numérique. Le projet repose sur la création d'un deepfake, c'est-à-dire un contenu vidéo réaliste généré par IA, dans lequel un avatar animé dispense le cours comme le ferait un enseignant humain. GPT-5 est utilisé pour rédiger un script structuré et précis, intégrant le contenu du chapitre et les instructions pour la scénarisation, tandis que HeyGen AI transforme ce script en vidéo en animant l'avatar et en générant une voix synthétique naturelle et multilingue si nécessaire. 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 souligne également les enjeux éthiques et techniques des deepfakes, notamment les risques de manipulation, la protection des droits à l'image et la nécessité d'une util-

isation responsable. 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 ouvrant une réflexion sur leurs limites et leur intégration sécurisée dans un contexte éducatif.

Toute somme, les différents travaux présentés ont mis en lumière l'évolution rapide des technologies numériques et cryptographiques, ainsi que leur impact majeur sur l'investigation et la pédagogie modernes. Du protocole ZK-NR, qui combine sécurité post-quantique, non-répudiation et opposabilité juridique, à l'usage de l'intelligence artificielle générative pour produire des contenus pédagogiques immersifs, il apparaît clairement que la convergence entre innovation technologique et exigences institutionnelles devient incontournable. Dans ce sens, ces recherches démontrent que la protection, l'authenticité et la fiabilité des données numériques ne sont plus de simples enjeux techniques, mais des éléments cruciaux pour garantir la confiance, la traçabilité et la recevabilité légale dans des contextes variés, qu'il s'agisse d'investigations judiciaires, de cybersécurité ou d'éducation. Enfin, elles soulignent également 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 robustes et de pratiques encadrées, afin d'assurer que l'innovation serve la société tout en préservant la sécurité, la confidentialité et l'intégrité des informations.