RÉPUBLIQUE DU CAMEROUN
*****
Paix – Travail – Patrie
*****
UNIVERSITÉ DE YAOUNDÉ I
*****
École Nationale Supérieure Polytechnique de Yaoundé
*****
Département de Génie Informatique
*****

REPUBLIC OF CAMEROON
*****
Peace – Work – Fatherland
*****
UNIVERSITY OF YAOUNDÉ I
*****
National Advanced School Engineering of Yaounde
*****
Computers Engineering Department
*****

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMERIQUE

THEME : L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA POLICE JUDICIAIRE

PAR :

NOMS & PRENOMS	FILIERE	MATRICULE
WANSI GILLES GILDAS	**HN-CIN-L4**	**22P037**

Sous la supervision de Ing THIERRY MINKA

Année Académique 2025/2026

Table des matières

1 L'UTILITE DE L'INVESTIGATION NUMERIQUE A LA POLICE JUDICIAIRE

L'analyse a démontré de manière éclatante que l'investigation numérique s'est imposée comme un outil indispensable au sein de la police judiciaire, et plus particulièrement dans le contexte camerounais. Face à une criminalité moderne qui a massivement migré vers le numérique, elle est passée du statut de compétence spécialisée à celui de pilier fondamental de toute enquête criminelle.

Notre réflexion a successivement mis en lumière ses apports essentiels – en faisant un instrument privilégié pour accéder à des preuves invisibles, identifier les auteurs et reconstituer des événements avec une précision inédite. Nous avons ensuite exploré la diversité de ses domaines d'application, de la lutte contre la cybercriminalité à la résolution des crimes violents en passant par le démantèlement des réseaux transnationaux, illustrant son utilité opérationnelle à travers de multiples affaires traitées sur le sol camerounais.

Cependant, cet exposé a aussi dressé un constat lucide : cet atout majeur se heurte à des défis et des limites substantielles. L'explosion du volume de données, la complexité technique croissante, les contraintes juridiques et les limites matérielles et humaines, notamment la pénurie d'experts et le coût des équipements, constituent des freins réels à son efficacité maximale au Cameroun.

Malgré ces obstacles, la trajectoire est tracée : il n'y a pas de retour en arrière possible. L'investigation numérique n'est plus une option, mais une nécessité pour la sécurité nationale et l'efficacité de la justice. Pour consolider ses acquis, le Cameroun doit impérativement investir dans la formation continue de ses enquêteurs, le renforcement des moyens logistiques des unités spécialisées et l'adaptation permanente de son cadre juridique.

En guise d'ouverture, l'avenir de l'investigation numérique s'annonce à la fois passionnant et périlleux. L'avènement de l'intelligence artificielle, l'utilisation croissante du métavers par les criminels, la menace des deepfakes pour la manipulation de preuves et les défis de l'ère post-quantique constituent les nouvelles frontières que la police judiciaire devra explorer. La capacité du Cameroun à anticiper ces mutations technologiques déterminera son succès dans la lutte contre la criminalité de demain.

Ainsi, loin d'être un simple outil technique, l'investigation numérique s'affirme comme un élément stratégique pour la souveraineté et la sécurité numérique de la nation.

2 PRÉSENTATION DÉTAILLÉE DU PROTOCOLE ZK-NR : RL ET POSITIONNEMENT DANS L'INVESTIGATION NUMÉRIQUE MODERNE

Le protocole ZK-NR (Zero-Knowledge Non-Répudiation) représente une avancée majeure dans l'investigation numérique moderne en conciliant sécurité cryptographique et exigences juridiques. Il répond au défi fondamental de la non-répudiation numérique, qui vise à empêcher qu'une partie ne nie avoir effectué une action (envoi, signature, transaction), tout en préservant la confidentialité des données sensibles.

Ce protocole s'appuie sur des preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs) permettant de vérifier l'authenticité et l'intégrité d'une preuve sans en révéler le contenu, combinées à des primitives cryptographiques post-quantiques comme les STARKs, Dilithium ou SPHINCS+ pour assurer une résilience face aux futures attaques quantiques.

Le ZK-NR s'inscrit dans un cadre théorique plus large, le Trilemme CRO, qui formalise l'impossibilité de satisfaire simultanément à un niveau optimal la Confidentialité (C), la Fiabilité (R) et l'Opposabilité juridique (O). Ce trilemme établit une borne d'impossibilité, contraignant les concepteurs à optimiser les compromis entre ces trois impératifs.

Pour y parvenir, l'architecture modulaire Q2CSI (Quantum-to-Classical Security Infrastructure) structure le protocole en couches distinctes – Fer (fiabilité), Or (confidentialité), Argile (opposabilité) – chacune supporté par des primitives spécialisées : la CEE (Chaotic Entropic Expansion) pour la confidentialité via une expansion entropique chaotique ; l'AOW (Affine One-Wayness) pour la fiabilité et la vérification temporelle ; et le SH (Semantic Holder) pour l'opposabilité juridique en assurant l'explicabilité des preuves. L'ensemble repose sur l'hypothèse cryptographique AIIP, garantissant la sécurité post-quantique du système.

Dans la pratique, ZK-NR répond directement aux besoins des enquêteurs numériques : garantir l'intégrité des preuves via une chaîne de possession (chain of custody) cryptographiquement scellée ; assurer la non-répudiation des actes grâce à des attestations vérifiables ; préserver la confidentialité des informations sensibles lors des investigations ; et renforcer l'opposabilité juridique des preuves produites, les rendant recevables devant les tribunaux.

Des cas concrets, comme des cyberfraudes bancaires ou des escroqueries BEC, illustrent la pertinence de ZK-NR face aux limites des méthodes traditionnelles (hachage simple, signatures RSA). En positionnant ZK-NR à la croisée de la cryptographie avancée et du droit, le document souligne que l'investigation moderne ne se limite plus à la collecte de preuves, mais exige de produire des attestations à la fois techniquement robustes et juridiquement incontestables.

Ainsi, ZK-NR incarne la convergence entre innovation cryptographique et exigence légale, ouvrant la voie à une nouvelle génération de preuves numériques adaptées à l'ère post-quantique.

3 LES DIX CAS AFRICAINS LES PLUS IMPORTANTS D'HACKING DE 2015 A 2025

Ce document présente une analyse approfondie de la cyber sécurité en Afrique à travers dix cas emblématiques d'hacking survenus entre 2015 et 2025, dans un contexte où la transformation numérique accélérée du continent s'accompagne d'une augmentation alarmante des cyber menaces - avec plus de 3 000 attaques hebdomadaires par organisation selon INTERPOL.

Les cas étudiés, sélectionnés selon une méthodologie rigoureuse d'investigation numérique en cinq étapes (identification, collecte, préservation, analyse technique et rapport) et évalués sur quatre critères (taille, type d'organisation, volume de données, impact), révèlent la diversité et la sophistication des attaques : du ransomware paralysant les ports sud-africains de Transnet (pertes : 60 millions USD) à la fuite massive

de données à la CNSS marocaine affectant 2 millions de salariés, en passant par les perturbations des systèmes électriques camerounais d'Eneo, le cyber-espionnage via Pegasus au Maroc, les piratages bancaires en Côte d'Ivoire (6 millions € détournés) et les fraudes au mobile money au Nigeria.

Ces incidents mettent en lumière les vulnérabilités structurelles du continent - infrastructures obsolètes, pénurie d'expertise locale, cadre juridique insuffisant - et soulignent l'urgence de mettre en œuvre les recommandations proposées : formation massive d'experts africains, création de CERT régionaux, harmonisation législative autour de la Convention de Malabo, développement d'un cloud souverain et renforcement de la gouvernance numérique, car l'avenir numérique de l'Afrique dépendra fondamentalement de sa capacité à bâtir une cyber souveraineté effective through une approche collaborative considérant la cyber sécurité comme une responsabilité partagée.

4 LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

Ce document présente une analyse comparative approfondie des trois meilleurs logiciels pour la rédaction de mémoire académique : Overleaf, Microsoft Word et Zotero, en mettant en lumière leurs spécificités, avantages et complémentarités.

Overleaf, éditeur LaTeX en ligne fondé en 2012 et racheté par Springer Nature, se distingue par sa qualité typographique professionnelle, sa gestion avancée des références croisées et sa collaboration en temps réel, bien qu'il présente une courbe d'apprentissage élevée, le rendant particulièrement adapté aux disciplines scientifiques et techniques où la précision formelle est cruciale.

Microsoft Word, outil universel de traitement de texte, demeure la solution la plus accessible grâce à son interface familière, sa gestion des styles hiérarchiques et sa compatibilité généralisée, mais il révèle des limites dans la gestion bibliographique avancée et peut montrer une instabilité sur les documents volumineux.

Zotero, gestionnaire de références bibliographiques open-source et gratuit, excelle dans la capture automatique des métadonnées, l'intégration transparente avec Word et Overleaf via des plugins dédiés, et le support de milliers de styles de citation, en faisant l'outil indispensable pour assurer la rigueur et l'exactitude des références.

La force de ces outils réside dans leur synergie : le duo Word + Zotero convient aux profils débutants ou en sciences humaines, la triade Overleaf + Zotero + ZoteroBib offre une excellence académique adaptée aux sciences exactes, et le workflow collaboratif Overleaf + Zotero Groups est idéal pour les travaux d'équipe ou les thèses.

Ainsi, la réussite d'un mémoire dépend moins du choix d'un outil unique que de l'adoption d'une combinaison stratégique qui allie qualité formelle, rigueur bibliographique et adaptabilité au profil de l'étudiant, tout en rappelant que ces logiciels, bien que sophistiqués, restent des instruments au service de la réflexion et de la profondeur intellectuelle.

5 POINTS SUR LES ALGORITHMES DE RECONNAISSANCE FACIALE

Ce document présente une analyse complète des algorithmes de reconnaissance faciale, en abordant à la fois leurs fondements techniques, leurs applications en investigation numérique, et les enjeux éthiques, juridiques et sociétaux qui les accompagnent.

La reconnaissance faciale, définie comme une technique biométrique non intrusive permettant d'identifier ou de vérifier l'identité d'une personne à partir de ses traits du visage, repose sur un système biométrique structuré en quatre modules : acquisition des données (via caméras ou scanners), extraction de caractéristiques (transformation en représentations mathématiques), correspondance (comparaison des vecteurs extraits avec une base de données) et décision (validation ou rejet de l'identité).

Les méthodes de reconnaissance se divisent en trois catégories principales : les méthodes globales (utilisant l'ensemble du visage, comme l'Analyse en Composantes Principales ou Eigenfaces), les méthodes locales (se concentrant sur des régions spécifiques comme les yeux ou la bouche, via des descripteurs tels que SIFT ou HOG) et les méthodes hybrides (combinant les avantages des deux approches pour une meilleure robustesse).

Les avantages de cette technologie incluent la rapidité de traitement, l'automatisation et la capacité à analyser de vastes volumes de données visuelles, ce qui en fait un outil précieux pour les enquêtes judiciaires et la cybersécurité. Cependant, elle présente également des limites significatives : sensibilité aux conditions réelles (lumière, angles), vulnérabilités aux attaques (deepfakes, injections adversariales), risques de biais (discrimination selon l'ethnie, le genre ou l'âge), et enjeux juridiques liés à la protection des données personnelles et au respect de la vie privée.

Pour encadrer son utilisation, le document propose des recommandations clés, telles que la documentation rigoureuse des pipelines techniques, la réalisation de tests locaux pour évaluer les performances, l'intégration de mécanismes anti-usurpation, la conduite d'études d'impact sur la vie privée, et l'adoption d'un cadre juridique aligné sur les lois nationales (comme la loi camerounaise sur les données personnelles).

En conclusion, la reconnaissance faciale représente un outil puissant pour l'investigation numérique, mais son déploiement doit être proportionné, transparent et supervisé pour concilier innovation technologique, sécurité et respect des droits fondamentaux.

6 DEEPFAKEVOCAL

Ce rapport explore en profondeur le phénomène du deepfake vocal, une technologie émergente d'intelligence artificielle qui permet de reproduire de manière quasi-indiscernable la voix humaine à partir d'échantillons audio limités.

Le document retrace l'évolution historique des deepfakes audio, depuis les premiers systèmes de synthèse vocale dans les années 1930 jusqu'à la révolution récente apportée par le deep learning avec des modèles comme WaveNet (2016) qui ont rendu le clonage vocal accessible et réaliste.

L'analyse distingue clairement les applications légitimes (accessibilité pour personnes handicapées, doublage audiovisuel, préservation patrimoniale) des utilisations malveillantes (escroqueries financières, usurpation d'identité, manipulation de l'opinion publique, falsification de preuves).

Le cas pratique de MINIMAX audio illustre concrètement comment ces technologies fonctionnent, démontrant la facilité avec laquelle on peut désormais cloner une voix et générer des discours fictifs. Les enjeux pour l'investigation numérique sont particulièrement critiques, car les deepfakes vocaux menacent directement le triptyque CRO (Confidentialité, Fiabilité, Opposabilité) des preuves audio, complexifient leur vérification et exigent une transparence méthodologique accrue.

Face à ces défis, le rapport propose plusieurs contre-mesures : développement d'outils de détection technologique, sensibilisation des utilisateurs, renforcement des cadres légaux, mise en place de méthodes d'authentification robuste et promotion d'une éthique stricte de l'IA.

En conclusion, le deepfake vocal représente à la fois une avancée technologique prometteuse et une menace sérieuse pour la confiance numérique, nécessitant une approche équilibrée entre innovation et régulation pour en maîtriser les impacts sociétaux.

7 CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK : CHOIX D'UNE NICHE DANS LE CADRE D'UNE INVESTIGATION NUMÉRIQUE

Ce rapport détaille la conception et l'analyse d'un faux profil TikTok créé dans le cadre d'une investigation numérique pédagogique, visant à étudier les mécanismes d'influence et d'engagement sur les réseaux sociaux tout en respectant un cadre éthique strict.

La niche choisie, la cybersécurité, s'est avérée stratégiquement pertinente car elle combine actualité, sensibilité aux enjeux numériques et potentiel éducatif, permettant d'aborder des thématiques concrètes comme la sécurité des mots de passe, les dangers du Wi-Fi public et les arnaques de phishing, illustrées par l'exemple fictif d'une fausse offre Orange Money.

Méthodologiquement, la création du profil s'est appuyée sur des outils préservant l'anonymat, notamment un service de messagerie temporaire, tandis que la stratégie de contenu privilégiait un ton léger et des visuels attractifs (via Canva et ChatGPT) pour maximiser l'engagement sans recourir à la tromperie malveillante.

L'analyse des réactions, suivie via TikTok Analytics, a révélé une audience réceptive, avec des publications atteignant jusqu'à 310 vues et générant des interactions significatives, confirmant l'efficacité d'une approche mêlant pédagogie et formats viraux.

Toutefois, le projet soulève des questions éthiques importantes concernant l'usage de faux profils, même à des fins éducatives, et met en lumière la fine frontière entre sensibilisation légitime et manipulation potentielle.

Les recommandations issues de cette expérience insistent sur la nécessité d'un encadrement strict des pratiques, l'intégration de la cybersécurité dans les curricula académiques et la promotion d'une culture numérique responsable, démontrant in fine que les réseaux sociaux constituent un terrain d'investigation fertile pour observer les comportements utilisateurs tout en diffusant des messages de prévention essentiels.

8 REALISATION D'UNE VIDEO À L'AIDE D'UNE IA OU UN INDIVIDU PRESENTE UN COURS

Ce projet académique illustre de manière concrète la réalisation d'une vidéo pédagogique utilisant l'intelligence artificielle générative, où un individu présente un cours sur les deepfakes grâce à l'utilisation combinée de GPT-5 et de HeyGen AI.

Le travail débute par une définition précise du deepfake, présenté comme un contenu médiatique falsifié créé via des techniques d'apprentissage profond, notamment les réseaux antagonistes génératifs (GAN) développés à l'origine par Ian Goodfellow en 2014, qui permettent grâce à l'entraînement mutuel de deux algorithmes (l'un générant des contrefaçons, l'autre les détectant) de produire des faux de plus en plus convaincants.

Le rapport souligne également les inconvénients et les préoccupations éthiques liés à cette technologie, notamment les risques d'atteinte à la vie privée et au droit à l'image, tout en évoquant les initiatives de régulation comme celles de la CNIL et les projets techniques de "désidentification" développés par Facebook.

La méthodologie de création repose sur une synergie d'outils : GPT-5, décrit comme un modèle de langage avancé d'Open AI capable de générer des textes cohérents et structurés, est utilisé pour produire le script détaillé du cours à partir du contenu du premier chapitre, tandis que HeyGen AI, plateforme spécialisée dans la synthèse vidéo, transforme ce script en une présentation audiovisuelle réaliste.

Le processus opérationnel avec HeyGen suit quatre étapes claires : sélection d'un template adapté, choix d'un avatar personnalisé, intégration du script généré par GPT-5 (avec ajustement de la voix, du ton et de la vitesse d'élocution) et finalement soumission pour génération rapide de la vidéo.

Les fonctionnalités remarquables de HeyGen mises en avant incluent la création d'avatars parlants ultra-réalistes, le clonage vocal permettant de reproduire fidèlement une voix humaine, et les capacités de traduction multilingue avec synchronisation labiale.

Cette expérience démontre avec efficacité le potentiel pédagogique de l'IA générative pour automatiser la production de contenus éducatifs immersifs, tout en alertant sur les limites techniques persistantes, les risques de manipulation et la nécessité impérative d'une approche éthique et régulée dans l'utilisation de ces technologies puissantes qui brouillent progressivement la frontière entre réalité et fiction.

9 SIMULATION D'UNE SERIE DE MESSAGES SUR WHATSAPP ENTRE UN HOMME ET SA MAITRESSE

Ce document est un rapport académique rédigé dans le cadre du cours "Théories et Pratiques de l'Investigation Numérique". Il a pour objet la simulation d'une série de messages WhatsApp entre un homme, Paul KENGNE (un enseignant), et sa maîtresse (une étudiante), dans le but d'étudier la falsification des preuves numériques.

Le travail ne porte pas de jugement moral mais vise à démontrer la facilité avec laquelle on peut créer des preuves numériques trompeuses et à en analyser les implications pour les enquêtes.

La méthodologie de falsification repose sur l'utilisation combinée de deux outils principaux. Le premier, Chatsmock, est une application web intuitive qui permet de générer des conversations WhatsApp réalistes en définissant les participants, le contenu des messages, les heures, les dates et les statuts de lecture. Il produit des captures d'écran qui imitent l'application réelle.

Le second outil, Adobe Photoshop, est utilisé dans un second temps pour parfaire le réalisme des images générées en corrigeant des détails graphiques (alignements, couleurs), en insérant des photos partagées dans la conversation (comme les "photos en tenue d'Adam" mentionnées) et en s'assurant que l'interface corresponde parfaitement à celle d'un smartphone, rendant la falsification difficile à détecter à l'œil nu.

Le rapport présente ensuite les limites de Chatsmock, notant un manque de réalisme sur certains détails d'interface, des fonctionnalités restreintes (incapacité à simuler des appels ou des notes vocales de manière convaincante), et le fait que le résultat final, étant une simple image, est susceptible d'être détecté par une analyse forensique experte cherchant des incohérences dans les métadonnées ou des anomalies graphiques.

Une comparaison avec d'autres outils comme FakeChat, WhatsFake ou l'usage direct de logiciels graphiques avancés est établie, concluant que la combinaison d'un générateur de conversation et d'un logiciel de retouche comme Photoshop permet d'atteindre un niveau de sophistication élevé.

L'impact de ces outils sur l'investigation numérique est majeur : ils entraînent une baisse significative de la fiabilité des captures d'écran présentées comme preuves, complexifient le travail des experts qui doivent désormais distinguer le vrai du faux avec des techniques avancées, et augmentent les risques de manipulation malveillante dans des contextes judiciaires ou disciplinaires, pouvant nuire à des réputations ou fausser des décisions.

Face à ces défis, le document émet plusieurs recommandations cruciales. Il préconise une vérification technique systématique des preuves, incluant l'analyse des métadonnées (horodatage, signature numérique). Il insiste sur la nécessité de sensibiliser et de former les acteurs judiciaires et administratifs (juges, avocats, enquêteurs) à la reconnaissance des falsifications.

L'utilisation d'outils spécialisés de détection de manipulations d'images est encouragée. Surtout, il recommande de privilégier les données brutes, c'est-à-dire l'extraction directe des messages depuis les bases de données des téléphones ou des serveurs, plutôt que de se fier à de simples captures d'écran, bien plus faciles à falsifier.

En conclusion, ce travail illustre de manière pratique la vulnérabilité des preuves numériques basées sur des images et souligne l'impérative nécessité pour l'investigation numérique d'évoluer en adoptant des méthodes de vérification rigoureuses et continues pour garantir l'intégrité et la fiabilité des preuves dans un paysage numérique où les outils de manipulation sont de plus en plus accessibles.