REPUBLIQUE 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 Yaoundé I
*****
NATIONAL ADVANCED SCHOOL OF ENGINEERING
*****
Computer Engineering Department
*****

SEC 4031 INTRODUCTION AUX TECHNIQUES D'INVESTTGATION NUMERIQUE

NOTES D'EXPOSES

Filière : HUMANITÉS NUMÉRIQUES

Niveau : IV

Rédigé par :

NGUEMO VOUFO AURELLE SANDRA 22P067 CIN4

Sous la supervision de :

Mr. MINKA

ANNEE ACADEMIQUE :2025-2026

RÉSUMÉ DU RAPPORT : CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK

Pour cet exposé en investigation numérique, un faux profil TikTok nommé Innotrends a été créé. L'objectif était d'étudier les mécanismes de viralité, d'engagement et de sensibilisation dans une niche ciblée sur la cybersécurité tout en respectant une démarche éthique et légale.

Création du profil :elle necessite l'utilisation d'une adresse email temporaire (Temp Mail) pour préserver l'anonymat.

Choix de la niche : la cybersécurité a été retenue pour son actualité, son utilité éducative et son adéquation avec les enjeux numériques actuels.

Stratégie de contenu : publication de six contenus éducatifs sur les mots de passe, Wi-Fi public, hameçonnage, empreinte numérique, etc.Avec l'utilisation des statistiques TikTok (vues, likes, partages) et tenue d'un tableau de bord pour le suivi des interactions.

Le profil a généré un engagement significatif (plus de 100 likes, jusqu'à 310 vues par publication). Les thématiques proches du quotidien (ex. : faux lien Orange Money) ont suscité intérêt et réactions. La bio percutante (« Découvre ce que les hackers ne veulent pas que tu saches ») a renforcé l'attractivité du compte.

on peut donc dire ici que La création d'un faux profil, même à visée pédagogique, soulève des questions éthiques (risque de tromperie, interprétation erronée des contenus). Nécessité d'un cadre strict pour éviter toute manipulation ou atteinte à la vie privée.

Et pour cela, nous devons renforcer l'éducation à la cybersécurité dès le secondaire. Promouvoir une utilisation responsable des réseaux sociaux et des outils numériques. Car ce projet a démontré l'efficacité des réseaux sociaux comme leviers de sensibilisation à la cybersécurité. Il souligne également l'importance d'allier innovation pédagogique et éthique numérique pour former des utilisateurs avertis et responsables.

RÉSUMÉ DU RAPPORT : DEEPFAKE VOCAL

Le deepfake vocal est une technologie d'intelligence artificielle permettant de reproduire ou d'imiter de façon quasi indiscernable la voix humaine à partir

d'enregistrements réels. Cette innovation, marquée par une évolution rapide depuis les premiers synthétiseurs jusqu'aux modèles de deep learning, offre à la fois des applications légitimes (accessibilité, doublage, assistants vocaux) et des usages malveillants (escroqueries, usurpation d'identité, manipulation de l'opinion). Les deepfakes audios ont connu une évolution croissante, depuis les premières machines à produire de la parole (Voder, 1939) jusqu'à la révolution du deep learning avec WaveNet (2016). La démocratisation des outils open-source a rendu le clonage vocal accessible au grand public.

Pour l'investigation numérique, les deepfakes vocaux représentent un enjeu majeur en menaçant le triptyque CRO (Confidentialité, Fiabilité, Opposabilité) des preuves audio. Ils complexifient la vérification et exigent une transparence accrue, tout en nécessitant une compréhension technique approfondie pour les enquêteurs.

Le cas pratique de MINIMAX audio illustre le clonage vocal de deux personnalités qui pourait etre utilise a desfins malveillante ou la falsification de preuves, pour prevenir cela il faut alors developper des outils d'analyse des signaux vocaux performant, et aussi former les utilisateus a recommaitre les deep fake vocaux. Le deepfake vocal représente à la fois une avancée technologique remarquable et un défi crucial pour la cybersécurité. Face aux menaces d'usurpation et de fraude, il devient impératif de développer des outils de détection fiables, de renforcer les cadres légaux et de promouvoir une éthique de l'intelligence artificielle pour orienter cette technologie vers un usage bénéfique et sécurisé.

RÉSUMÉ DU RAPPORT : SIMULATION DE MESSAGES WHATSAPP

Dans cet exposé il nous est présenté un travail pratique réalisé dans le cadre du cours, ayant pour objectif de démontrer la facilité avec laquelle il est possible de falsifier des preuves numériques, en particulier des conversations WhatsApp. L'exercice s'appuie sur la simulation d'une conversation adultère

entre un enseignant, Paul KENGNE, et son etudiante, afin d'illustrer les risques de manipulation dans un contexte judiciaire ou disciplinaire.

Mise en situation Le scénario retenu met en scène un enseignant marié entretenant une relation secrète avec une étudiante. Les échanges simulés incluent des messages affectifs, des propos explicites, des promesses de quitter l'épouse légitime Mme judith Kengne, ainsi que l'envoi de photos intimes. Pour reproduire ces conversations de manière crédible, deux outils principaux ont été utilisés :

Chatsmock : une application web permettant de générer de fausses discussions WhatsApp en personnalisant les noms, les photos de profil, les heures et le statut de lecture.

Adobe Photoshop : utilisé pour parfaire le réalisme des captures en retouchant les détails graphiques (alignement, couleurs, insertion d'images). L'association de ces outils a permis de produire des visuels quasi identiques à de véritables captures d'écran, démontrant ainsi la simplicité technique de fabriquer des preuves trompeuses, mais il présente certaines limites : un réalisme imparfait sur certains détails d'interface, des fonctionnalités restreintes (pas de simulation d'appels ou de messages vocaux), et une exportation limitée au format image. D'autres outils comme FakeChat ou WhatsFake offrent des options similaires mais manquent également de crédibilité face à une analyse experte. En revanche, l'usage d'un logiciel comme Photoshop permet un niveau de falsification bien plus avancé et difficile à détecter, bien qu'il exige des compétences techniques supérieures.

De ce fait la fiabilité des captures d'écran comme preuve est remise en cause, les experts doivent développer des compétences avancées pour identifier les falsificationsLes risques de manipulation judiciaire et de diffamation sont accrus.

Pour y faire face, il faut une vérification technique systématique : analyse des métadonnées, signatures numériques et origine des fichiers, sensibiliser les acteurs judiciaires et administratifs aux risques de falsification, une utilisation d'outils forensiques spécialisés pour détecter les manipulations. Privilégier les données brutes (extraction directe depuis les bases de données) plutôt que les captures d'écran.

RÉSUMÉ DU RAPPORT : PRESENTATION DES ALGORITME DE RECONNAISSANCE FACIALE

La reconnaissance faciale est une technologie biométrique d'identification qui repose sur l'analyse des traits du visage. Son fonctionnement suit un processus en trois phases (enrôlement, identification, vérification) et s'appuie sur différentes méthodes algorithmiques, allant des approches classiques (globales, locales, hybrides) aux techniques modernes de deep learning. Bien que cet outil offre des avantages opérationnels significatifs en investigation numérique – notamment la rapidité de traitement de grands volumes d'images – il présente également des limites techniques, des vulnérabilités face aux attaques adversariales, et des risques importants en matière de protection des données.

Au-delà des aspects techniques, la reconnaissance faciale soulève des enjeux éthiques, juridiques et sociétaux majeurs, tels que le respect de la vie privée, les risques de discrimination algorithmique et la nécessité d'un encadrement légal. Pour un déploiement responsable, il est essentiel de mettre en place des mesures de sécurité renforcées, des audits réguliers, une validation humaine des décisions critiques, et de veiller à la proportionnalité des usages, particulièrement dans un contexte judiciaire ou de sécurité publique. En tant qu'investigateur numérique, la reconnaissance faciale représente un outil stratégique dans les enquêtes judiciaires et la cybersécurité. Elle permet de traiter rapidement de grands volumes d'images et de vidéos souvent collectés dans des contextes sensibles (surveillance de lieux publics, preuves numériques extraites d'appareils saisis, etc.) pour identier ou conrmer l'identité de personnes. Ainsi, la présentation de cette technologie ne se limite pas à la description technique des algorithmes : elle intègre aussi une réexion sur leur ecacité opérationnelle, leurs limites face aux tentatives de dissimulation ou d'usurpation, et sur leur utilisation responsable dans le respect des cadres juridique et éthique en vigueur , sans encadrement clair, audits techniques, transparence et gouvernance adaptée, cette technologie peut générer des dérives graves : faux positifs judiciaires, atteintes à la vie privée, discriminations, contestations légales ou déance sociale. En revanche, lorsqu'elle est contrôlée, contextualisée et accompagnée de procédures rigoureuses, la reconnaissance faciale peut devenir un atout majeur pour les enquêtes judiciaires et la cybersécurité.

RÉSUMÉ DU RAPPORT : PRESENTATION DES LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE MÉMOIRE

Ce document présente une analyse comparative de trois logiciels essentiels pour la rédaction académique : Overleaf, Microsoft Word et Zotero. Overleaf, éditeur LaTeX en ligne, offre une qualité typographique professionnelle et une gestion avancée des références, idéal pour les disciplines scientifiques, malgré une courbe d'apprentissage élevée. Microsoft Word, outil universel et accessible, facilite la rédaction et la collaboration, mais présente des limites dans la gestion bibliographique. Zotero, gestionnaire de références open-source, permet une collecte, organisation et citation automatisée des sources, garantissant rigueur et conformité aux normes académiques.

L'efficacité optimale réside dans la combinaison de ces outils selon le profil et les besoins : Word + Zotero pour les débutants, Overleaf + Zotero pour l'excellence scientifique, et Overleaf + Zotero Groups pour les projets collaboratifs. Aucun logiciel seul ne couvre tous les besoins ; c'est leur synergie qui permet de concilier qualité formelle, rigueur méthodologique et efficacité, sans pour autant négliger l'importance du fond et de la réflexion intellectuelle dans la réussite du mémoire.En dénitive, cette analyse démontre que la réussite d'un mémoire repose en grande partie sur le choix stratégique d'outils logiciels adaptés. Chaque solution présente des atouts complémentaires : Overleaf excelle par sa qualité typographique irréprochable et son approche structurante, idéale pour les documents complexes. Microsoft Word conserve son avantage majeur en termes d'accessibilité et de prise en main immédiate, grâce à son interface universellement connue. Quant à Zotero, il apporte la rigueur bibliographique indispensable à tout travail académique sérieux, en automatisant la gestion des références avec une précision inégalée. Notre recommandation principale s'oriente vers la combinaison Overleaf + Zotero, qui ore le meilleur équilibre entre qualité professionnelle, rigueur scientique et ecacité, particulièrement adaptée aux exigences des mémoires de master et thèses. Pour autant, n'oublions pas que ces outils, aussi sophistiqués soient-ils, ne demeurent que des instruments au service de la pensée. L'importance de maîtriser ses outils est indéniable, mais il serait dommageable de négliger le fond au prot de la forme. La plus belle mise en page et la bibliographie la plus impeccable ne sauraient compenser un contenu faible ou une réexion

insusante. L'étudiant averti saura donc trouver le juste équilibre entre la perfection technique et la substance intellectuelle, entre la maîtrise de l'outil et la profondeur de la recherche.

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

Cet exposé présente le protocole ZK-NR (Zero-Knowledge Non-Repudiation), une architecture cryptographique modulaire visant à garantir la non-répudiation qui est le fait de s'assurer qu'un contrat, notamment un contrat signé via internet, ne peut être remis en cause par l'une des parties. Dans le domaine de la sécurité des systèmes d'information, la non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues. tout en préservant la confidentialité des données. Il s'appuie sur des primitives post-quantiques (STARKs, signatures BLS à seuil, Dilithium) et s'inscrit dans le cadre théorique du Trilemme CRO, qui établit l'impossibilité de satisfaire simultanément Confidentialité, Fiabilité et Opposabilité juridique. Les composants CASH (CEE, AOW, SH) permettent de minimiser cette incompatibilité en offrant respectivement confidentialité, vérification temporelle et explicabilité juridique.

Le ZK-NR répond aux besoins de l'investigation numérique moderne en garantissant l'intégrité des preuves, la traçabilité des actions et la résilience face aux attaques quantiques. Il permet de produire des attestations vérifiables sans divulguer d'informations sensibles, renforçant ainsi l'opposabilité légale des preuves. Des cas pratiques (cyberfraude, SIMBOX, EncroChat) illustrent son applicabilité dans des enquites réelles, positionnant le ZK-NR comme une avancée majeure pour concilier sécurité cryptographique et exigences judiciaires. L'évolution de la cryptographie, de simple outil de protection des communications à instrument d'opposabilité juridique, transforme profondément le champ de l'investigation numérique. Désormais, les enquêteurs ne cherchent pas seulement à sécuriser ou à cacher les informations,

mais à produire des preuves authentiques, vérifiables, inaltérables et légalement recevables. Les protocoles comme ZK-NR, les cadres comme CLO, ainsi que les primitives post-quantiques, ouvrent la voie à une nouvelle génération de pratiques forensiques où la preuve numérique devient incontestable devant un tribunal. Ainsi, l'investigation numérique moderne ne se limite plus à collecter des données, mais s'inscrit dans une démarche intégrée où la cryptographie devient le garant de la vérité numérique..

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

Ce document analyse l'utilité de l'investigation numérique au sein de la police judiciaire, en particulier dans le contexte camerounais. Il démontre que cette discipline est devenue un outil indispensable pour accéder à des preuves invisibles dans le monde physique, lutter contre la cybercriminalité, identifier et tracer les auteurs, reconstituer des événements et produire des preuves recevables en justice. Ses applications sont vastes, couvrant la criminalité financière, la grande criminalité transfrontalière, le terrorisme, les crimes violents et la protection de l'enfance, comme l'illustrent plusieurs affaires résolues au Cameroun.

Cependant, le déploiement de l'investigation numérique se heurte à des défis majeurs, notamment l'explosion du volume des données, l'évolution technologique rapide, des contraintes juridiques et un cadre législatif à parfaire. Le Cameroun fait également face à des limites pratiques, telles qu'une pénurie d'experts certifiés, la centralisation des compétences, et des contraintes matérielles et financières importantes. Malgré ces obstacles, l'investigation numérique s'impose comme un pilier stratégique pour la sécurité nationale, nécessitant des investissements soutenus en formation, en équipement et en adaptation du cadre légal pour relever les défis futurs comme l'IA et les deepfakes.