REPUBLIQUE DU CAMEROUN

Paix – Travail – Patrie

****

UNIVERSITE DE YAOUNDE I

****

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

****

DEPARTEMENT DE GENIE INFORMATIQUE

REPUBLIC OF CAMEROON

Peace – Work – Fatherland

****

UNIVERSITY OF YAOUNDE I

****

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

****

DEPARTMENT OF COMPUTER ENGINEERING

Résumé expose

Investigation numérique dans un milieu en constante évolution

---

Participant : TAPA loic

Superviseur : Ing. Thierry Minka

Année Académique : 2025–2026

Table des matières

Introduction

L'ère numérique marque une transformation profonde des sociétés, des institutions et des relations humaines. Au Cameroun comme ailleurs, la numérisation des services, le développement des infrastructures internet, l'extension des transactions financières en ligne et la généralisation des smartphones ont multiplié les opportunités, mais aussi les risques.

Selon Kaspersky, le nombre d'exploits de cybersécurité au Cameroun est passé de ** 174 472 en 2023** à ** 333 930 en 2024**, soit une augmentation d'environ **91

Ce document se veut une étude détaillée de l'investigation numérique : ses outils, ses défis, ses pratiques, ses implications légales, ses techniques avancées comme les deepfakes ou la cryptographie post-quantique, et des recommandations adaptées au contexte camerounais.

—

1 Logiciels de rédaction, gestion des preuves et collaboration

1.1 Besoins spécifiques dans un contexte académique et judiciaire

- Fiabilité, rigueur dans les citations, respect des normes bibliographiques.
- Conservation des versions, traçabilité des modifications (important pour preuves).
- Sécurité, confidentialité, sauvegarde fiable des documents.

1.2 Outils principaux

1.2.1 Microsoft Word + Zotero / Mendeley

Avantages : large use, interface graphique, nombreux modèles. Limites : gestion poussée des équations ou schémas complexes moins bonne, problèmes de compatibilité.

1.2.2 Google Docs

Très utile pour collaboration en temps réel, édition partagée, propositions de modifications. Cependant, dépendance à la connexion Internet, risque de fuite si partage non sécurisé.

1.2.3 LaTeX + Overleaf

Excellence pour documents scientifiques : formules, figures, gestion de bibliographie via BibTeX ou BibLaTeX. Permet versionnage, export PDF fiable. Inconvénient : courbe d'apprentissage, besoin de configuration (packages, styles), moins intuitif pour débutants.

1.3 Gestion des preuves numériques

1.3.1 Format des preuves

Captures d'écran, métadonnées, logs, fichiers originaux, horodatage, hash (SHA-256, etc.), intégrité.

1.3.2 Chaîne de conservation (Chain of Custody)

Principe, documentation, scellage, précautions lors de copies, procédures légales au Cameroun (lois, accord judiciaire, normes).

1.4 Recommandations pratiques

— Toujours garder l'original des preuves et des copies horodatées.

— Utiliser des services de stockage sécurisés, chiffrés.

— Sensibilisation à la gestion des documents : métadonnées, suppression des données sensibles.

—

2 Analyse approfondie des cybermenaces au Cameroun

2.1 Statistiques globales

En 2024, les exploits de sécurité (vulnérabilités exploitées) au Cameroun ont augmenté de 91

2.2 Typologie des cybermenaces

1. **Scamming / arnaque en ligne** : promesses frauduleuses, faux agents bancaires, faux sites, etc.
2. **Phishing** : emails, SMS, sites usurpés.
3. **Usurpation d'identité** : vol de données personnelles, usurpations de profil.
4. **Intrusions, attaques RDP, backdoors** : accès non autorisé à des systèmes. :contentReference[oaicite :22]index=22

5. **Vol de données / fuites** : institutions publiques ou privées dont les systèmes sont compromis.
6. **Attaques DDoS** : perturbations de service. Exemple : plusieurs compagnies de télécommunications en Cameroun touchées en 2024. :contentReference[oaicite :23]index=23

2.3 Impact financier et social

— Pertes estimées à **6 milliards FCFA** pour le Cameroun en 2019 à cause de cyberfraud. :contentReference[oaicite :24]index=24

— Perte cumulée de plusieurs milliards de FCFA pour les banques et institutions suite à phishing, scamming, usurpation d'identité. :contentReference[oaicite :25]index=25

— Effet sur la confiance du public, sur le commerce en ligne, sur les transactions bancaires.

— Impact sur les infrastructures critiques (énergie, télécoms) en cas d'attaques importantes comme DDoS ou intrusions. Exemple Eneo en 2024. :contentReference[oaicite :26]index=26

2.4 Réponse nationale / cadre légal

— Le Cameroun a adhéré à la **Convention de Budapest sur la cybercriminalité** en décembre 2023. :contentReference[oaicite :27]index=27

— L'ANTIC mène des campagnes de sensibilisation, des formations. :contentReference[oaicite :28]index=28

— Existence de lois nationales sur la cybercriminalité, mais défis pour leur mise en œuvre : manque de moyens, de personnel spécialisé, de sensibilisation.

—

3 Reconnaissance faciale, biométrie et implications légales

3.1 Principes techniques

— Détection de visage (MTCNN, Viola-Jones, etc.).

— Extraction des traits : distance pupilles, contours, traits discriminants.

— Modèles de classification / identification : Eigenfaces, Fisherfaces, CNNs.

— Entraînement sur des bases de données (problème de biais de données si représentation non africaine).

3.2 Cas d'utilisation au Cameroun

— Identification dans les aéroports pour la sécurité ou le contrôle des passeports.

— Banques ou institutions financières utilisant reconnaissance faciale pour authentification.

— Projets gouvernementaux de biométrie dans registres d'état civil ou cartes nationales.

3.3 Risques et cadre légal

— Vie privée, consentement, droits fondamentaux.

— Biais algorithmique : visages africains souvent sous-représentés dans datasets, ce qui entraine plus d'erreurs.

— Légalité des usages : nécessité de fondements légaux, autorisation judiciaire, respect des conventions internationales.

—

4 Deepfake : types, mécanismes, détection

4.1 Typologie des deepfakes

— Deepfake image / face swap.

— Deepfake vidéo (mouvements, expression, synchronisation).

— Deepfake vocal (synthèse de voix, clonage).

— Deepfake audio-vidéo combiné.

4.2 Mécanismes techniques

— GANs (Generative Adversarial Networks).

— Modèles de synthèse vocale : Tacotron 2, WaveNet, etc.

— Apprentissage multimodal et transfert de style.

4.3 Outils et benchmarks récents

— *DeepfakeBench* : benchmark unifié, 15 méthodes, 9 datasets. :contentReference[oaicite :29]index=29

— *Deepfake-Eval-2024* : collecte «in the wild», perte de performance des modèles de détection sur ce type de données. :contentReference[oaicite :30]index=30

— Outils de détection audio : *Resemble Detect*. :contentReference[oaicite :31]index=31

4.4 Stratégies de détection et de prévention

— Vérification des métadonnées, recherche de cohérence audio-vidéo, spectrogrammes.

— Watermarking (marque imperceptible) dans médias authentiques.

— Authentification des plateformes, chaînes de confiance.

— Sensibilisation des utilisateurs : reconnaître les anomalies visuelles ou auditives (lip-sync, artefacts, etc.).

—

5 Cryptographie post-quantique : protocoles, usages et défis

5.1 Pourquoi post-quantique ?

— Les ordinateurs quantiques, quand ils seront matures, pourront casser certains schémas cryptographiques actuels (RSA, ECC) via algorithmes comme Shor.

— Le NIST a engagé un processus de standardisation d'algorithmes résistants. :contentReference[oaicite :32]index=32

— Les Etats-Unis, l'UE commencent déjà à adopter ces nouveaux algorithmes. :contentReference[oaicite :33]index=33

5.2 Quelques protocoles et schémas

— PQXDH (Post-Quantum Extended Diffie-Hellman) : combinant Kyber (post-quantum) avec ECC pour assurer compatibilité. :contentReference[oaicite :34]index=34

— CECPQ1 : expérimentation TLS avec NewHope + X25519. :contentReference[oaicite :35]index=35

— Algorithmes retenus par le NIST (exemples : CRYSTALS-Kyber, Dilithium, etc.).

5.3 Défis spécifiques pour le Cameroun et l'Afrique

— Ressources limitées (coût, infrastructures, personnel formé).

— Intégration dans les systèmes existants (banques, gouvernements).

— Standardisation locale, compatibilité légale et réglementaire.

— Sensibilisation et confiance du public.

—

6 Investigation numérique via réseaux sociaux et OSINT

6.1 OSINT : définitions et méthodes

Recherche d'informations publiques (réseaux sociaux, forums), analyse de métadonnées, scrapping, cartographie des connexions.

6.2 Faux profils, géolocalisation, métadonnées

Comment créer un profil fictif à des fins légales, comment tracer une localisation (IP, GPS des posts), horodatage, captures d'écran, authentification.

6.3 Cas camerounais / africains

Exemple : escroqueries sur TikTok liées à promesses de gains rapides, ou faux influenceurs. Analyse des hashtags crypto, giveaway, etc.

—

7 Rôle judiciaire, preuves électroniques et lois

7.1 Cadre légal au Cameroun

Loi sur la cybercriminalité, adhésion à conventions internationales, rôle de l'ANTIC, du ministère de la Justice.

7.2 Preuves électroniques : chaîne de conservation, authenticité

Horodatage, hash, métadonnées, copies légales, forensic numérique.

7.3 Exemples de cas d'usage

Jugements ou décisions au Cameroun ou jurisprudence impliquant preuves numériques, cyberfraude bancaire, cas d'usurpation, etc.

—

8 Solutions, recommandations et perspectives

8.1 Solutions techniques

— Renforcement des systèmes de sécurité (patchs, firewalls, détection d'intrusions).

— Adoption de la cryptographie post-quantique dans les infrastructures critiques.

— Déploiement d'outils de détection de deepfake adaptés au contexte local.

8.2 Recommandations institutionnelles

— Formation des magistrats, policiers, enquêteurs en numérique.

— Renforcement du cadre légal, accélération de l'adhésion aux conventions internationales.

— Coopération internationale et partage d'informations.

8.3 Perspectives futures

Impact de l'IA générative, réglementation des contenus synthétiques, évolution des menaces, évolution technologique (quantique, edge computing), rôle de l'éducation numérique.

—

Conclusion

L'investigation numérique est essentielle pour affronter les défis modernes de la cybersécurité, de la désinformation, et de la protection des droits individuels. Le Cameroun a déjà des structures (ANTIC, etc.), mais doit renforcer ses capacités techniques, légales et éducatives. L'avenir passe par des systèmes robustes, transparents et adaptés au contexte local, notamment en ce qui concerne les deepfakes et la cryptographie post-quantique.

—

Bibliographie

— Kaspersky. (2025). Rapport sur l'augmentation de 91

— ANTIC. Articles sur les cyberfraudes, phishing, usurpation d'identité au Cameroun. :contentReference[oaicite :37]index=37

— DeepfakeBench. (2023). Benchmark de détection des deepfakes. :contentReference[oaicite :38]index=38

— Deepfake-Eval-2024. (2025). Benchmark «in the wild» de deepfakes récents. :contentReference[oaicite :39]index=39

— Article "Le chiffrement est entré dans l'ère postquantique". Le Monde, 2025. :contentReference[oaicite :40]index=40

— Résemble Detect et outils de détection audio. :contentReference[oaicite :41]index=41

— D'autres publications nationales et internationales sur la cybercriminalité, les lois, les cas judiciaires, etc.