Résumé des différents exposés

HEYA SALOMON CIN-4

October 2025

1 Résumé : Points sur les algorithles de reconnaissance faciale

La reconnaisance faciale est un outil issu de l'intelligence artificielle d'identifier ou de vérifier l'identité d'une personne à de traits visage spécifiques tels que: la distance entre les yeux, la forme du nez, les contours de la mâchoire ou des lèvres. Son système (le système biomètrique) se compose de 4 modules à savoir:

- La capture ou acquisition
- l'Extraction de caractéristiques
- La correspondance
- La décision

Elle comprend plusieurs méthodes à savoir

- Méthodes globales : elles utilisent l'ensemble des visages comme source d'information, sans se focaliser sur des traits particuliers.
- Méthodes locales : elles extraient des caractéristiques à partir de régions spécifiques (yeux, bouches, nez) et utilise la géométrie ou leurs apparences comme données.
- Méthode hybrides : elles combinent des approches locales et globales afin d'unir leurs avantages.

En conclusion la reconnaissance faciale est un outil technologique puissant pour l'investigation numérique, permettant d'exploiter rapidement de vastes volumes d'images et de vidéos dans des contextes sécuritaires, judiciaires ou de prévention

2 Résumé : Simulation d'une série de message sur whatsapp entre

Les échanges numériques occupent une place centrale dans la vie sociale et personnelle, les applications de messagerie comme whatsapp constituent une source d'information priviligiée mais aussi un vecteur de manipulation Des nombres personnes utilisent ces outils que sont les réseaux sociaux à des fins malveillantes tels que :

la création de fausses preuves incriminants un individu ainsi que la désinformation, de ce fait l'investigateur numérique doit toujours chercher à vérifier l'authenticité des éléments en sa disposition. Ainsi des mesures préventives sont nécessaires telles que:

- Vérification technique des preuves : qui consisite à l'analyse des métadonnées et fichiers (signatures numérique, origine) afin de confirmer leur authenticité
- Sensibilisation des acteurs judiciaires et administratifs : former les juges, avocats, magistrats à la reconnaiisance des falsifications numériques
- Utilisation d'outils spécialisés : le recours à des logiciels de détection de manipulation d'images et d'analyses forensiques
- Préference pour les données brutes : privilègier la récupération directe des messages depuis les bases de données des téléphones ou des serveurs, plutôt que de simples captures d'écran
- Renforcement du cadre légal : établir des règles précises sur l'acceptabilité des preuves numériques devant les juridictions.

Des outils tels que Chatsmock et Adobe Photoshop ont permis de montrer à quel point il est simple de créer des preuves numériques trompeuses. Cette pratique mets en évidence la fragilité des éléments de preuve issus des applications de messagerie instantanée, particulièrement lorsque ceux ci se limitent à des simples captures d'écran.

3 Résumé : Deepfake

Un deepfake en français faux profond selon Fortinet est une forme d'intelligence artificielle qui peut être utilisée pour créer des images, sons et des vidéos de canulars convaincants. Parmi les innovations les plus marquantes figure le deepfake, un procédé qui permet de générer des images, des vidéos ou des sons artificiels d'un réalisme saisissant. Les deepfakes audios sont utilisés selon deux cadres, notamment le cadre légitime et le cadre malveillant:

- Applications légitimes et bénéfiques:

  - Accessibilité et inclusion : offrir une voix naturelle aux personnes ayant perdu l'usage de la parole (patients atteints de SLA, laryngectomisés, etc.)
  - Doublage et production audiovisuelle : accélérer le doublage multilingue de films et séries sans dénaturer le jeu d'acteur original
  - Assistants virtuels et interfaces vocales : rendre les interactions plus fluides, natu relles et personnalisées
  - Préservation des voix : conserver la voix d'artistes ou de proches disparus à des fins mémorielles ou patrimoniales

- Applications malveillantes et criminelles :
  - Escroqueries et fraudes financières : imitation vocale d'un responsable hiérarchique ou d'un proche pour tromper un interlocuteur et obtenir des transferts d'argent
  - Usurpation d'identité et chantage : utilisation de clones vocaux pour contourner des systèmes d'authentification ou piéger des victimes
  - Manipulation de l'opinion publique : diffusion de faux discours ou d'enregistrements fabriqués pour influencer des événements politiques ou sociaux.
  - Falsification de preuves numériques : création d'audios truqués susceptibles d'être présentés comme des preuves dans des enquêtes, des procès ou des conflits

Contre-mesures et moyens de prévention contre le deepfake vocal Face aux menaces posées par le clonage vocal, plusieurs solutions émergent et doivent être appliquées :

- Détection technologique Développement d'outils capables d'analyser les signaux vocaux pour identifier des anomalies propres aux voix générées par IA.
- Sensibilisation et éducation Les utilisateurs doivent être formés pour reconnaître les risques.
- Cadre légal et réglementaire Plusieurs pays réfléchissent à des lois spécifiques sur les deepfakes, imposant des sanctions et un marquage numérique (watermarking) des contenus générés.

il ressort que le deepfake vocal incarne à la fois une avancée technologique remarquable et un défi majeur pour la cybersécurité et l'investigation numérique.

4 CONCEPTION ET ANALYSE D'UN FAUX PROFIL TIKTOK

À l'ère où les réseaux sociaux façonnent l'opinion, influencent les comportements et redéfinissent les interactions humaines, TikTok s'impose comme une plateforme incontournable, notamment auprès des jeunes générations cette investigation numérique, réalisée à travers la création d'un faux profil TikTok dans le cadre d'un projet pédagogique, nous a permis d'explorer de manière concrète les pratiques liées à la sensibilisation à la cybersécurité. L'expérience a également mis en lumière l'importance d'une approche éthique, encadrée et réfléchie, dans ce type d'exercice. La maîtrise des outils digitaux, combinée à une conscience critique des impacts possibles, s'impose aujourd'hui comme un socle essentiel pour tout acteur du numérique.

5 LES TROIS MEILLEURS LOGICIELS DE RÉDACTION DE M

La rédaction d'un mémoire représente un dé académique majeur, tant par son ampleur que par sa complexité. Entre la gestion fastidieuse des sources bibliographiques, lerespect des normes formelles et la structuration d'un contenu substantiel, l'étudiant se trouve confronté à une entreprise qui dépasse largement le cadre de la simple rédaction. Dans ce contexte exigeant, le choix des outils logiciels devient un paramètre déterminant pour la réussite du projet. Overleaf se dé nit comme un éditeur LaTeX en ligne collaboratif qui a révolutionné l'approche de la rédaction académique. Sa philosophie repose sur trois piliers fondamentaux :

- L'accessibilité : rendre LaTeX utilisable sans installation complexe
- La collaboration : permettre un travail d'équipe uide et synchronisé
- La qualité : maintenir les standards professionnels de l'édition scientique

La plateforme se distingue par plusieurs atouts décisifs pour la rédaction d'un mémoire :

- Qualité typographique exceptionnelle : Production automatique de documents au rendu professionnel, avec un placement optimal des gures, une justication parfaite et une hiérarchie typographique claire
- Gestion avancée des références croisées : Système robuste pour les renvois aux figures, tables, équations et chapitres, avec numérotation et mise à jour automatiques.
- Collaboration en temps réel : Partage instantané avec le directeur de mémoire, fonction de commentaires intégrée et historique des modifications

- Modèles académiques prêts à l'emploi : Bibliothèque de templates conformes aux exigences des universités et revues scientiques

6 Les 10 cas africains les plus d'important d'hacking durant ces 10

La cybersécurité africaine se trouve aujourd'hui à un carrefour stratégique. L'accélération de la numérisation touche tous les secteurs : télécommunications, énergie, santé, administration, éducation, transport et finance. Cependant, la plupart des pays du continent manquent encore d'une infrastructure solide pour protéger leurs systèmes critiques, Plusieurs facteurs expliquent cette vulnérabilité :

- Faible maturité institutionnelle : la plupart des États ne disposent pas encore de lois complètes sur la cybersécurité.
- Manque de compétences locales : en moyenne, on compte moins d'un expert en cybersécurité pour 100 000 habitants
- Infrastructures obsolètes : de nombreux systèmes d'information reposent sur des logiciels non mis à jour.
- Dépendance extérieure : hébergement de données à l'étranger, ce qui rend les États dépendants de prestataires non africains.

Les principales menaces observées sont :

- Les ransomwares (rançongiciels) qui chiffrent les données contre rançon
- Les fraudes au mobile money et aux systèmes bancaires
- L'espionnage numérique à des fins politiques

L'investigation numérique s'articule autour de cinq étapes fondamentales :

- Identification de l'incident : détection précoce de l'attaque et définition du périmètre.
- Collecte des preuves : acquisition des données à partir des disques, serveurs, journaux et réseaux.
- Préservation de l'intégrité : copies forensiques, hachage et stockage sécurisé.
- Analyse technique : utilisation d'outils spécialisés (Autopsy, FTK, EnCase, Wireshark).
- Rédaction du rapport : documentation rigoureuse, utile aux juridictions et aux décideurs.

7 L'UTILITÉ DE L'INVESTIGATION NUMÉRIQUE DANS LA

L'investigation numérique (ou digital forensic) est une discipline qui consiste à collecter, analyser, conserver et présenter des preuves numériques issues d'ordinateurs, de téléphones, de réseaux ou de tout autre support électronique, dans le but d'appuyer une enquête (judiciaire, administrative ou privée).

Les apports essentiels de l'investigation numérique à la police judiciaire :

- Accès à des preuves invisibles dans le monde physique : L'investigation numérique permet de retrouver des traces difficiles à effacer : historiques de navigation, conversations supprimées, métadonnées, fichiers effacés mais récupérables.
- Lutte contre la cybercriminalité: Les enquêtes sur le piratage informatique, les fraudes en ligne, les ransomwares, le phishing reposent directement sur ces techniques
- Identification et traçage des auteurs: Analyse des adresses IP, des journaux système, des connexions réseaux permettent de remonter jusqu'au suspect.
- Reconstitution des événements : L'investigation permet de reconstituer une chronologie numérique :
- Quand un fichier a été créé, modifié, transféré?
- À quelle heure un utilisateur s'est connecté?
- Quelles données ont été effacées ou copiées

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

Le protocole ZK-NR (Zero-Knowledge Non-Repudiation) est une architecture cryptographique modulaire en couches, axée sur la non-répudiation préservant la confidentialité pour la co-production de services numériques publics. Il combine des primitives post-quantiques (STARKs, signatures BLS à seuil, Dilithium) pour créer des preuves sécurisées, vérifiables et surtout auditables, sans jamais révéler de contenu sensible. L'écosystème scientifique et industriel autour des preuves à divulgation nulle de connaissance (Zero-Knowledge), de la cryptographie post-quantique et de l'investigation numérique est porté par plusieurs pôles de recherche et d'innovation

- Pôle A : Zero-KnowledgeetSTARKs
- Pôle B : Cryptographie Post-Quantique: La cryptographie post-quantique s'impose comme une priorité face aux menaces posées par l'ordinateur quantique.
- Pôle C : Sécurité Formelle et Composabilité : Cepôle, davantage théorique, concerne la sécurité formelle et la composabilité.
- Pôle D : Investigation Numérique et Opposabilité Juridique : Le lien entre cryptographie et investigation numérique se manifeste dans les travaux de Eoghan Casey, auteur de l'ouvrage de référence Digital Evidence and Computer Crime, qui a largement contribué à définir les standards de la preuve numérique dans les enquêtes judiciaires.
- Pôle E : Projets et Entreprises : Plusieurs entreprises et projets jouent également un rôle moteur. StarkWare incarne la traduction industrielle des STARKs, en travaillant sur la scalabilité et la mise en production de ces preuves dans l'écosystème blockchain.
- Pôle F : Groupes Académiques et Industriels : . Dans le domaine post-quantique, les groupes impliqués dans le développement de CRYSTALS, FALCON, HQC et SPHINCS+ représentent une force collective d'innovation