الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي

Université Abou Bekr Belkaid
Tlemcen Algérie

جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

FACULTÉ DES SCIENCES
DÉPARTEMENT D'INFORMATIQUE

Mémoire

Pour
L'obtention du diplôme de
MASTER en Informatique
Option : Réseaux et Systèmes Distribués (RSD)

Présenté par
Mlle : FEROUI Nadia

THÈME

Protection contre des photos en zone non autorisée

Soutenu en Octobre 2023 devant un jury composé de

Mr BENMOUNA Youcef	Président
Mr BELABED Amine	Examinateur
Mr TADLAOUI Mohamed	Expert
Mr BELHOCINE Amine	Encadreur
Mr KROMBA Brahim	Co-encadreur

Remerciement

Je tiens particulièrement à remercier le tout Miséricordieux, le tout puissant, ce mémoire n'aurait jamais été réalisé sans sa bénédiction

Je tiens à exprimer mes remerciements à mes encadreurs, Monsieur BELHOCINE Amine et Monsieur KROMBA Brahim, pour leur aide constante, leurs conseils avisés et leurs remarques objectives.

Je remercie les membres du jury, Monsieur BENMOUNA Youcef d'avoir l'amabilité de présider le jury, Monsieur BELABED Amine et Monsieur TADLAOUI Mohamed d'avoir accepté d'examiner mon travail.

Je profite de cette opportunité pour exprimer ma gratitude à Monsieur SOULIMANE Sofiane et au centre I2E qui ont contribué par leur collaboration, disponibilité et sympathie

Enfin, je tiens à remercier les clubs CI2E, SCORPIO, et toute personne qui m'a aidée de près ou de loin durant mon travail et en particulier tous mes amis.

Dédicaces

A mes très chers parents Aucun hommage ne pourrait être à la hauteur de l'amour et de l'affection dont ils ne cessent de me combler. Que Dieu leur procure bonne santé et longue vie.

A mes chères sœurs Sarah et Samia.

A ma nièce et mon beau-frère Lilya et Chakib.

A tous mes amis surtout CHERIF BENMOUSSA Bachir, a tous ceux que j'aime et qui m'aiment.

Table de matières

Liste des figures

Résumé

Introduction Générale……1

CHAPITRE I : Notions sur la protection de la vie privée

1. La vie privée……4
1.1. Les types de vie privée……...5
1.2.Les types de confidentialité……5
1.3. L'hypothèse de la vie privée……6
1.4. La protection de vie privée……6
1.5. Normes partagées pour l'évaluation des technologies de sécurité de l'information et de protection de la vie privée……8
2. Désidentification et désidentification irréversible……..9
2.1 Classification des identifiants dans les contenus multimédias……9

CHAPITRE II : solution pour la désidentification

1.Désidentification des identifiants non biométriques……12
1.1 Texte……...12
1.2 Coiffure et du style vestimentaire..……..12
1.3 Plaques d'immatriculation……..…13
2. Désidentification des identifiants biométriques physiologiques……....13
2.1 Visages dans les images fixes……..…13
2.2 Visages dans les systèmes de vidéosurveillance…….…14
2.3 Empreintes digitales……..15
2.4 L'iris……..17
2.5 L'oreille……..…17
3. Les systèmes de protection……...18
4. Désidentification des identifiants biométriques comportementaux……..19
4.1 La démarche et des gestes……..19
5. Désidentification des identifiants biométriques souples……....19
5.1. La silhouette du corps……20
5.2. Cicatrices, marques et tatouages……21

CHAPITRE III : Application et Résultat

1.Environnement de travaille……24
1.1 Environnement matériel…….……24
1.2 Environnement Logiciel……..24
2. Le langage utilisé pour le développement…..……...24
3. Analyse et Conception de l'application……....25
3.1 Diagramme de cas d'utilisation…….25
3.2 Diagramme de séquence……25
3.3 Création de l'application……27
L'appareil photo……....27
La géolocalisation……29
L'authentification…….…….31
4.Zone Rouge……32
5.zone orange……34
6.zone verte……...35
7.Conclusion……..37
Conclusion générale…….38
BMC : Business Model Canvas……..40
1.Proposition de Valeur……41
2. Segment de Marché……..41
3. Relation Client……..41
4. Canaux de Distribution…….42
5. Partenaires Clés……42
6. Activités Clés……42
7. Ressources Clés……43
8. Structure de Coûts……43
9. Source de Revenus et Modèle de Prix……..44
Bibliographie……45

Liste des figures :

Figure I.1. Vie privée connotations.....5

Figure I.2 Aperçu conceptuel du projet projet CareMedia.....7

Figure I.3. Taxonomie des identificateurs dans le contenu multimédia.....10

Figure II.1. Méthodes naïves de désidentification des visages : a) Image originale ; b) Flou : σ2= 18 ; c) Pixellisation : paramètre p = 12 14

Figure II.2. Désidentification k-Same : a) image originale, b) image désidentifiée pour k=6.....14

Figure II.3. Mélange d'empreintes digitales : a) empreinte originale ; b) fonction de transformation -empreinte d'un doigt différent ; c) nouvelle image d'empreinte digitale mélangée qui masque l'identité de l'empreinte originale.....16

Figure II.4. Une image vidéo d'exemple est à gauche. Le résultat du système est affiché dans l'image de droite, où le visage de l'homme au gilet vert est masqué. Le reste de la scène, y compris les visages des travailleurs qui ne portent pas de gilets verts, reste visible…….18

Figure II.5. Résultat de la dépersonnalisation de la silhouette du corps par la méthode de brouillage décrite dans.....21

Figure II.6. Désidentification des tatouages ; a) Exemple d'une image fixe obtenue par un appareil photo couleur ; b) Caractéristiques SIFT extraites ; c) Image fixe de tatouage désidentifiée …….....21

Figure III.1 Diagramme de cas d'utilisation……..25

Figure III.2 Diagramme de séquence…….26

Figure III.3.Dépendances pour caméra……...27

Figure III.4. Application Flutter de visualisation de la caméra en temps réel……27

Figure III.5. Traitement d'Image : Floutage en Flutter……28

Figure III.6. Dépendance de la géolocalisation……..29

Figure III.7. Une carte personnalisées dans google my maps……29

Figure III.8.(a) et (b) :Intégrer une Carte Google My Maps en Flutter…….30

Figure III.9.Dépendances pour l'authentification…….31

Figure III.10.Vérification de l'authentification dans Flutter……...31

Figure III.11. Caméra en temps réel avec prise de photo…….32

Figure III.12. Image flouté……33

Figure III.13. Interface d'authentification…….34

Figure III.14.a) Capture d'image en direct depuis la caméra ; **b)** Photo capturée……....36

Résumé

Les applications de confidentialité et de protection de la vie privée sont des outils conçus pour aider les utilisateurs à contrôler les informations qu'ils partagent en ligne. Deux techniques courantes utilisées pour protéger la vie privée sont le floutage et la géolocalisation. Le floutage est une technique qui consiste à rendre floues certaines parties d'une image ou d'une vidéo pour protéger l'identité des personnes qui y figurent. Par exemple, les visages peuvent être floutés pour empêcher leur identification, ou les plaques d'immatriculation peuvent être floutées pour empêcher la reconnaissance d'un véhicule. Cette technique est souvent utilisée par les médias pour protéger la vie privée des personnes impliquées dans des événements sensibles, tels que des témoins de crimes ou des victimes d'accidents. La géolocalisation est une technique qui permet de déterminer la position géographique d'un utilisateur à l'aide de son appareil mobile ou d'un autre dispositif de localisation. Cette technique peut être utile pour fournir des informations géographiques précises, mais elle peut également poser des problèmes de confidentialité si elle est utilisée de manière abusive. Par exemple, si une application utilise la géolocalisation pour suivre les déplacements d'un utilisateur sans son consentement, cela peut constituer une violation de sa vie privée.

Mot clés : Protection, Vie privée, Multimédia, floutage,géolocalisation,confidentialité.

Abstract

Privacy and data protection applications are tools designed to help users control the information they share online. Two common techniques used to safeguard privacy are blurring and geolocation. Blurring is a technique that involves making certain parts of an image or video blurry to protect the identity of individuals featured in them. For example, faces can be blurred to prevent identification, or license plates can be blurred to prevent the recognition of a vehicle. This technique is often employed by the media to safeguard the privacy of individuals involved in sensitive events, such as crime witnesses or accident victims. Geolocation is a technique used to determine a user's geographical position using their mobile device or another location-tracking device. This technique can be helpful for providing precise geographical information, but it can also raise privacy concerns if misused. For instance, if an app uses geolocation to track a user's movements without their consent, it can be a violation of their privacy.

Keywords : Protection, Privacy, Multimedia, blurring, geolocation, confidentiality.

ملخص

تعتبر تطبيقات الخصوصية وحماية البيانات أدوات مصممة لمساعدة المستخدمين في السيطرة على المعلومات التي يشاركونها عبر الإنترنت. تُستخدم تقنيتان شائعتان لحماية الخصوصية، وهما التشويش وتحديد الموقع الجغرافي. التشويش هو تقنية تتضمن جعل أجزاء معينة من صورة أو فيديو غامقة لحماية هوية الأفراد الظاهرين فيها. على سبيل المثال، يمكن تشويه الوجوه لمنع التعرف على الشخص، أو يمكن تشويه لوحات السيارات لمنع التعرف على المركبة. تُستخدم هذه التقنية غالبًا من قبل وسائل الإعلام لحماية خصوصية الأفراد المشاركين في أحداث حساسة، مثل شهود الجرائم أو ضحايا الحوادث. تقنية تحديد الموقع الجغرافي هي تقنية تُستخدم لتحديد الموقع الجغرافي للمستخدم باستخدام جهازه المحمول أو جهاز تتبع موقع آخر. يمكن أن تكون هذه التقنية مفيدة لتوفير معلومات جغرافية دقيقة، ولكنها قد تثير أيضًا مخاوف بشأن الخصوصية إذا تم استخدامها بشكل سيء. على سبيل المثال، إذا استخدم تطبيق تحديد الموقع الجغرافي لتتبع حركات المستخدم دون موافقته، يمكن أن يكون ذلك انتهاكًا لخصوصيته.

الكلمات المفتاحية: الحماية، الخصوصية، الوسائط المتعددة، عدم الوضوح، تحديد الموقع الجغرافي، السرية.

Introduction Générale

L'essor d'Internet et des technologies de l'information a considérablement modifié la façon dont nous communiquons, travaillons et interagissons avec le monde qui nous entoure. Cependant, en échange de ces avantages, nous avons également vu une augmentation des risques relatifs à la confidentialité et à la protection de la vie privée en ligne.

Aujourd'hui, de nombreuses personnes partagent des informations personnelles en ligne sans vraiment comprendre les conséquences potentielles de leurs actions, ce qui peut entraîner des violations de la vie privée, des atteintes à la sécurité et des risques pour la sécurité. En réponse à ces préoccupations, des entreprises et des développeurs ont créé des applications et des outils pour aider les utilisateurs à protéger leur vie privée en ligne.

Parmi ces outils, le floutage et la géolocalisation sont des techniques courantes utilisées pour protéger la vie privée. Le floutage permet de rendre floues certaines parties d'une image ou d'une vidéo pour protéger l'identité des personnes qui y figurent, tandis que la géolocalisation permet de déterminer la position géographique d'un utilisateur à l'aide de son appareil mobile ou d'un autre dispositif de localisation.

Dans cette optique, cette discussion portera sur l'application de ces techniques pour protéger la vie privée en ligne, leur fonctionnement et leur importance dans la protection de la vie privée.

Le floutage est une technique de protection de la vie privée couramment utilisée dans les médias pour flouter les visages, les plaques d'immatriculation ou d'autres informations sensibles dans les images et les vidéos. Cette technique est souvent utilisée pour protéger l'identité des personnes impliquées dans des événements sensibles, tels que des témoins de crimes ou des victimes d'accidents. En floutant ces parties, il est plus difficile pour les autres de les identifier ou de les localiser, préservant ainsi leur vie privée.

Le floutage est généralement effectué avec des logiciels de retouche d'image spécialisés qui permettent de flouter les parties sélectionnées de l'image ou de la vidéo. Il existe également des applications mobiles qui permettent aux utilisateurs de flouter rapidement et facilement les parties sensibles de leurs photos avant de les partager en ligne.

Quant à la géolocalisation, elle est souvent utilisée pour fournir des informations géographiques précises, telles que la localisation d'un magasin ou d'un restaurant. Cependant, elle peut également poser des problèmes de confidentialité si elle est utilisée de manière abusive. Par exemple, certaines applications peuvent utiliser la géolocalisation pour suivre les déplacements d'un utilisateur sans son consentement, ce qui peut constituer une violation de sa vie privée.

Pour aider à protéger la vie privée en ligne, de nombreuses applications et outils intègrent des fonctionnalités de géolocalisation qui permettent aux utilisateurs de contrôler les informations qu'ils partagent. Par exemple, certaines applications peuvent permettre aux utilisateurs de désactiver la géolocalisation ou de limiter l'accès à leur position géographique à certaines personnes ou à certains moments.

En conclusion, le floutage et la géolocalisation sont deux techniques importantes pour protéger la vie privée en ligne. Le floutage permet de protéger l'identité des personnes dans les images et les vidéos, tandis que la géolocalisation peut être utilisée pour fournir des informations géographiques précises tout en préservant la vie privée des utilisateurs. Il est important de comprendre comment ces techniques fonctionnent et de les utiliser de manière responsable pour protéger la vie privée en ligne.

CHAPITRE I :

Notions sur la protection de la vie privée

La vie privée est l'un des problèmes sociaux et politiques les plus importants de notre société de l'information, caractérisée par une gamme croissante de technologies et de services habilitant et de soutien. Parmi ceux-ci figurent les communications, le multimédia, la biométrie, le big data, le cloud computing, l'exploration de données, Internet, les réseaux sociaux et la surveillance audio-vidéo. Chacun d'entre eux peut potentiellement fournir les moyens d'une intrusion dans la vie privée. L'anonymisation est l'une des principales approches de la protection de la vie privée dans les contenus multimédias (texte, images fixes, séquences audio et vidéo et leurs combinaisons).

1. La vie privée :

Il n'existe pas de définition unique du terme "vie privée". La signification de la vie privée dépend des contextes juridiques, politiques, sociétaux, culturels et socio-technologiques [1]. D'un point de vue juridique, la première définition de la vie privée a été donnée par Louis D. Brandeis et Samuel D. Warren il y a plus de 120 ans [2]. Ils ont défini la vie privée comme "le droit d'être laissé seul", en ce qui concerne l'acquisition et la diffusion d'informations concernant la personne, en particulier par le biais de publications, de photographies ou d'autres médias non autorisés. En outre, selon Brandeis et Warren, la personne doit être protégée contre les enquêtes et les saisies qui envahissent une sphère de solitude individuelle jugée raisonnable par la société. En outre, la personne a le droit d'être laissée seule en ce qui concerne les décisions fondamentales relatives à ses relations intimes ou aux aspects de sa vie.[65]

Alan F. Westin définit la vie privée comme la prétention d'un individu à déterminer quelles informations le concernant doivent être connues des autres [3]. Sur la base des différentes utilisations du mot "vie privée", il existe de nombreuses conceptions différentes de la vie privée et elles peuvent être classées en six types généraux [4] :

(i) Le droit d'être laissé seul ;

(ii) L'accès limité à soi - la capacité de se protéger contre l'accès non désiré des autres ;

(iii) Le secret - la dissimulation de certaines choses aux autres ;

(iv) Le contrôle des informations personnelles ;

(v) La personnalité - la protection de la personnalité, de l'individualité et de la dignité de l'individu ;

(vi) Intimité - contrôle ou accès limité aux aspects intimes de la vie.

1.1. Les types de vie privé :

En fonction des contextes sociaux et/ou des situations de la vie réelle, la vie privée, en général, peut être divisée en un certain nombre de concepts distincts, mais liés [5] :

(i) La vie privée informationnelle - le droit de l'individu de limiter l'accès aux informations personnelles qui pourraient être utilisées de quelque manière que ce soit pour identifier un individu ;

(ii) La vie privée intentionnelle - le droit de l'individu d'empêcher ou d'interdire la communication ultérieure d'informations observées par l'individu ;

(iii) La vie privée décisionnelle - le droit de l'individu à prendre des décisions concernant sa vie sans ingérence indue ;

(iv) La vie privée spatiale - le droit de l'individu à disposer de ses propres espaces personnels qui ne peuvent être violés sans son consentement explicite.

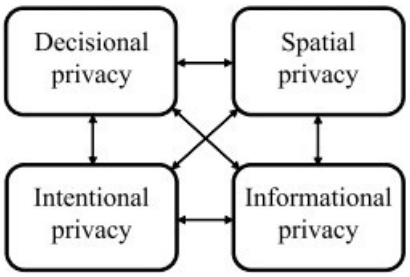


Figure I.1. Vie privée connotations [5]

1.2 Les types de confidentialité :

Si nous incluons certains contextes physiques et socio-technologiques dans la classification ci-dessus, nous pouvons parler de :

(i) La confidentialité des informations, qui implique l'établissement de règles régissant la collecte et le traitement des données personnelles telles que les dossiers médicaux et fiscaux et les informations de crédit ;

(ii) La confidentialité des communications, qui couvre la sécurité et la confidentialité du courrier, du téléphone, du courrier électronique et d'autres formes de communication ;

(iii) La confidentialité du corps, qui concerne la protection de l'intégrité physique des personnes contre les procédures invasives telles que les tests génétiques, les tests de dépistage de drogues et les fouilles à corps ;

(iv) La confidentialité territoriale, qui concerne la fixation de limites à l'intrusion dans les environnements domestiques et autres, tels que le lieu de travail ou l'espace public. Cela inclut les fouilles, la vidéosurveillance et les contrôles d'identité.[65]

1.3 L'hypothèse de la vie privée :

L'ouvrage [4] offre une vue approfondie et complète de la théorie de la vie privée, des tentatives existantes pour la conceptualiser, et des différentes définitions de la vie privée, abordées par des juristes, des philosophes et des sociologues. Il illustre la nécessité de protéger la vie privée et les données personnelles grâce à trois exemples de violations de la vie privée.

Le premier cas concerne une personne dont la vie privée a été compromise après qu'une caméra de vidéosurveillance l'a enregistrée en train de se tailler les veines dans une rue. Les images ont été diffusées sans son consentement, ce qui a conduit à une bataille judiciaire pour violation de la vie privée, finalement gagnée par la victime.

Le deuxième cas concerne un voleur d'identité qui a utilisé des informations volées pour souscrire à des contrats de téléphonie mobile et obtenir des smartphones. L'Agence de protection des données personnelles a découvert des irrégularités, et le voleur a été arrêté.

Le troisième cas concerne l'utilisation de la reconnaissance faciale sans consentement lors d'un événement sportif. Cette violation a entraîné l'interdiction de l'utilisation de la reconnaissance faciale dans les lieux publics pour éviter les abus potentiels.

Les violations de la vie privée décrites dans ces cas pourraient être évitées par la dépersonnalisation des identifiants biométriques et des mesures de sécurité appropriées pour les informations personnelle

1.4 La protection de la vie privé :

Le vol, la modification et le partage des gabarits biométriques posent des risques pour la vie privée et la sécurité. Trois aspects sont cruciaux pour protéger la vie privée des individus en ce qui concerne ces gabarits [6] :

i) L'irréversibilité : Il doit être informatiquement difficile de reconstituer le gabarit biométrique original à partir des données de référence stockées.

ii) L'impossibilité de lier différents gabarits biométriques entre eux ou avec la personne source.

iii) La confidentialité : Le gabarit biométrique doit être protégé contre tout accès ou divulgation non autorisée.

Récemment, des efforts ont été déployés pour normaliser la protection des gabarits biométriques, et quatre principaux systèmes de protection ont émergé [6] :

i) L'extraction et le stockage d'une esquisse mathématique du gabarit biométrique.

ii) L'engagement flou, où un vecteur de caractéristiques biométriques est associé à un message secret.

iii) Le cryptage des caractéristiques biométriques lors de l'inscription.

iv) La biométrie annulable ou révocable, où le gabarit est transformé à l'inscription à l'aide d'une transformation secrète, et la reconnaissance est basée sur la correspondance avec un modèle de test obtenu en utilisant la transformation correcte.

La biométrie annulable s'applique à diverses modalités biométriques, telles que les données faciales, empreintes digitales, iris, voix…etc. Des détails exhaustifs sur la biométrie annulable et les systèmes cryptographiques biométriques sont disponibles dans [7, 8].

Les questions de confidentialité, d'éthique et de législation liées à la confidentialité dans divers contextes et environnements sont examinées en détail [9, 10]. [9] explore la protection de la vie privée basée sur l'obscurcissement cryptographique réversible. De plus, [10] analyse les questions de protection de la vie privée dans les scénarios de surveillance multimédia, comme la surveillance audio et vidéo, soulignant la nécessité d'obtenir un mandat pour une surveillance légale. [10] se penche sur les implications éthiques de la surveillance multimédia en temps réel dans les établissements de soins de longue durée, tout en notant la nécessité de dépersonnaliser les données sensibles pour protéger la vie privée. Cependant, il souligne la vulnérabilité potentielle des participants si la dépersonnalisation n'est pas effectuée immédiatement après la collecte des données.

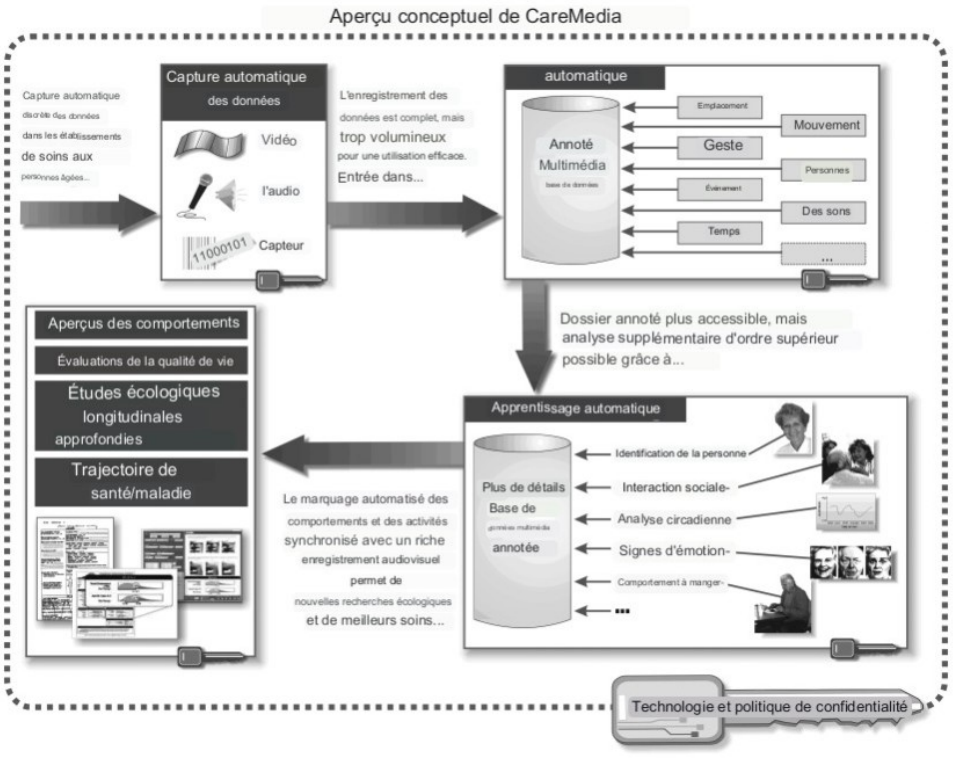


Figure I.2 Aperçu conceptuel du projet projet CareMedia[10]

1.5 Normes partagées pour l'évaluation des technologies de sécurité des technologies de l'information et de protection de la vie privée :

Le respect de la vie privée est intrinsèquement lié à la protection de la vie privée, et ces aspects sont fortement influencés par les technologies dédiées à la sauvegarde de la vie privée. Le socle de référence est constitué par la norme multipartite "Critères communs pour l'évaluation de la sécurité des technologies de l'information" [11], ainsi que les technologies visant à renforcer la protection de la vie privée [12, 13].

Ces technologies de protection de la vie privée sont conçues pour sécuriser les données personnelles stockées, potentiellement intrusives, et sont intégrées dans l'environnement des technologies de l'information et de la communication (TIC). Leur rôle consiste à réduire ou éliminer les données personnelles, prévenir leur traitement inutile ou non désiré, tout en préservant les fonctionnalités des systèmes d'information [12].

L'extension de ces technologies a donné naissance à une approche plus substantielle appelée "Privacy by Design" (PbD), initiée dans les années 90 [14]. Cette approche combine les principes des pratiques équitables en matière d'information avec une démarche proactive pour intégrer la protection de la vie privée dans les spécifications de conception des technologies, des pratiques commerciales et des infrastructures physiques.

Pour faciliter la compréhension, voici quelques définitions clés [65] :

(i) Les informations personnelles englobent toutes les données relatives à un individu.

(ii) Les informations personnelles identifiables (ou identifiants personnels) sont des données personnelles permettant d'identifier une personne.

(iii) Les problèmes de protection de la vie privée surgissent dès que des informations personnelles contenant des identifiants personnels sont capturées dans un contenu multimédia, comme du texte, des images statiques, des séquences audio et vidéo, ou leur combinaison.

(iv) Pour préserver la vie privée des individus capturés dans un contenu multimédia, il est impératif de dépersonnaliser tous leurs identifiants personnels. Nous utilisons le terme "reconnaissance d'un identifiant personnel" pour désigner l'identification ou la vérification biométrique d'une personne sur la base de ses identifiants personnels. Par exemple, la reconnaissance d'un portail signifie l'identification ou la vérification d'une personne selon sa démarche. Les technologies informatiques modernes, telles que la biométrie, l'informatique en nuage, l'intelligence ambiante, l'exploration de données, les services Internet, les réseaux sociaux et la surveillance audio-vidéo, peuvent porter atteinte à la vie privée en permettant la collecte, l'extraction, l'observation, le transfert et le stockage d'identifiants personnels.

2. Désidentification et désidentification irréversible

La dépersonnalisation des contenus multimédias est définie comme le processus consistant à dissimuler ou à supprimer les identifiants personnels, ou à les remplacer par des identifiants personnels de substitution dans les contenus multimédias, afin d'empêcher la divulgation et l'utilisation des données à des fins sans rapport avec l'objectif pour lequel l'information a été obtenue à l'origine. Il ne fait aucun doute que la dépersonnalisation est l'une des méthodes de base pour protéger la vie privée, tout en permettant d'autres utilisations des informations personnelles.

Les termes "dépersonnalisation" et "anonymisation" sont souvent utilisés de manière interchangeable, mais certains experts font la différence entre les deux. La dépersonnalisation est le processus réversible qui consiste à supprimer ou à masquer toute information personnellement identifiable dans les dossiers individuels, de manière à minimiser le risque de divulgation involontaire de l'identité des personnes et des informations les concernant. Il s'agit de fournir des informations supplémentaires pour permettre l'extraction des identifiants d'origine, par exemple par un organisme autorisé. L'anonymisation fait référence au processus de dépersonnalisation des données qui produit des données dont les enregistrements individuels ne peuvent pas être reliés à un original car ils ne contiennent pas les variables de traduction nécessaires pour ce faire [15]. Il s'agit d'un processus unidirectionnel (irréversible) qui ne permet pas d'obtenir les identifiants originaux à partir des données dépersonnalisées. Dans le présent document, nous utilisons le terme "dé-identification" pour les deux approches, mais dans certains cas, nous soulignons s'il s'agit d'un processus réversible ou irréversible. Dans les deux cas, le processus de désidentification doit être suffisamment efficace, que les tentatives de reconnaissance soient effectuées par des humains ou par des machines. En outre, dans de nombreux cas, le processus de dépersonnalisation doit également préserver l'utilité, le caractère naturel et l'intelligibilité des données [16, 17].

2.1 Classification des identifiants dans les contenus multimédias

La taxonomie des identifiants dans les contenus multimédias nécessitent une dépersonnalisation pour protéger la vie privée, s'inspirant de l'approche Safe Harbour [18]. Cette approche identifie 18 types d'identifiants à dépersonnaliser pour garantir la confidentialité des bénéficiaires de soins de santé, notamment les noms, les sous-divisions géographiques, les dates spécifiques, les numéros de téléphone, les adresses électroniques, les numéros de sécurité sociale, et bien d'autres.Ces identifiants peuvent être regroupés en deux catégories : les identifiants non-biométriques (tels que le contexte textuel, vocal, les plaques d'immatriculation, le contexte socio-politique, le style vestimentaire) et les identifiants biométriques, qui sont des caractéristiques distinctives et permanentes. Les identifiants biométriques comprennent des aspects physiologiques (comme le visage, l'iris, l'empreinte digitale) et des caractéristiques comportementales (comme la voix, la démarche, le geste).

Il est à noter que les identifiants biométriques souples englobent des caractéristiques physiques, comportementales ou adhérentes, moins distinctives. Ils ne sont pas suffisants pour une identification fiable mais peuvent améliorer les performances de la reconnaissance. La désidentification multimodale implique la dépersonnalisation simultanée des identifiants biométriques, biométriques logiciels et non biométriques.

La détection et la dissimulation des identifiants personnels dans les contenus multimédias constituent un défi interdisciplinaire, impliquant des domaines scientifiques tels que le traitement du langage naturel, le traitement des images, la reconnaissance des formes, l'apprentissage automatique, l'analyse de la parole, le suivi vidéo et la biométrie.[65]

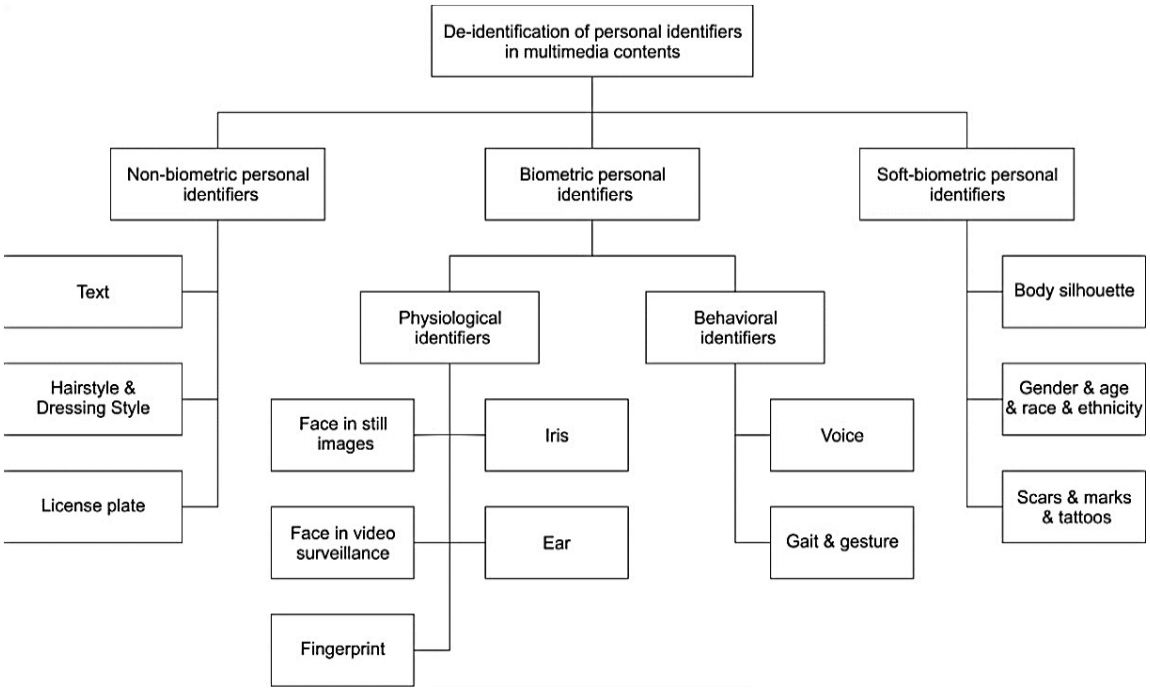


Figure I.3. Taxonomie des identificateurs dans le contenu multimédia.[18]

CHAPITRE II :
solution pour la désidentification

Dans cette partie, nous donnons un aperçu de la désidentification des identifiants non biométriques, des identifiants biométriques physiologiques, des identifiants biométriques comportementaux et des identifiants biométriques souples. Outre les solutions de désidentification, nous discutons également des problèmes non résolus et des défis liés à la désidentification, à l'évaluation du niveau de protection de la vie privée, au caractère naturel et à l'utilisabilité des contenus multimodaux désidentifiés.

1. Désidentification des identifiants non biométriques :

1.1 Texte :

La recherche sur la dépersonnalisation a débuté avec les dossiers médicaux personnels (DMP) basés sur du texte. Dans ce domaine, la dépersonnalisation signifie retirer certaines informations spécifiques du fichier texte et les remplacer par des données fictives, généralement réalistes. Cette pratique est largement automatisée et repose sur des modèles, des connaissances spécialisées, ou des combinaisons de dictionnaires et d'algorithmes de traitement du texte. Des méthodes d'apprentissage automatique, d'heuristiques, de statistiques, et d'appariement de motifs sont également employées.[19]

La dépersonnalisation réversible est couramment utilisée pour protéger les données personnelles dans les domaines de la santé et de la recherche médicale [20]. L'imagerie médicale, qui inclut des informations d'en-tête et des données d'image, contient des informations sensibles pour la vie privée, comme la reconstruction du visage à partir de modèles tridimensionnels issus de tomodensitométrie (CT) et d'imagerie par résonance magnétique (MR)[21].

Pour garantir la protection de la vie privée, les informations sensibles dans l'en-tête DICOM (Digital Imaging and Communications in Medicine) doivent être supprimées ou remplacées par des données fictives, tandis que les données d'image doivent être dépersonnalisées à l'aide de filtres de confidentialité réversibles.

1.2 Coiffure et style vestimentaire :

La manière dont une personne se coiffe et s'habille peut en dire beaucoup sur son identité, et ces éléments peuvent être utilisés pour classer les individus dans des catégories distinctes. De plus, il existe un défi appelé "contrainte par paire" d'identification, où les gens peuvent déduire que deux visages dépersonnalisés dans une vidéo appartiennent à la même personne en se basant sur des éléments tels que les vêtements, la coiffure, le style vestimentaire, ou d'autres indices alternatifs. Cela comporte un risque de révélation de l'identité des personnes[22].

Les informations alternatives qui peuvent contribuer à révéler l'identité incluent le contexte

du discours, le contexte social et politique, ainsi que l'environnement. Malheureusement, il y a eu relativement peu de recherches consacrées à la suppression ou à la dissimulation de la coiffure, du style vestimentaire, et des éléments mentionnés ci-dessus pour la dépersonnalisation des données[23].

1.3 Plaques d'immatriculation :

Des services web comme Google Street View et EveryScape collectent et partagent d'énormes quantités d'images de lieux publics. Ces images contiennent des informations sensibles pour la vie privée, comme les visages des gens et les numéros de plaque d'immatriculation des voitures. Selon l'approche Safe Harbour, ces données sont parmi les 18 types d'identifiants qui doivent être dépersonnalisés pour protéger la vie privée.[65]

Dans un article [24], les chercheurs se sont concentrés sur la détection des visages et des plaques d'immatriculation dans les images de Google Street View. Pour la dépersonnalisation, ils ont simplement flouté les zones détectées. Ils ont utilisé une méthode simplifiée pour détecter les plaques d'immatriculation, basée sur une analyse rapide de fenêtres de différentes tailles. Cette méthode combine différents types de détecteurs de caractéristiques, allant des caractéristiques simples et rapides aux caractéristiques plus coûteuses mais plus informatives. Ils ont indiqué qu'un système entièrement automatique a réussi à détecter et flouter environ 94 à 96 % des plaques d'immatriculation dans les images de Google Street View.

Dans un autre article [25], les chercheurs ont proposé une méthode appelée "inhomogeneous principal component blur (IPCB)" pour flouter de manière adaptative les pixels des plaques d'immatriculation en fonction de la distribution préalable des informations sensibles. Cette méthode cherche à équilibrer la protection de la vie privée et la préservation de la qualité en ne floutant que la partie de la plaque contenant les numéros d'immatriculation, laissant d'autres parties intactes, comme le nom de l'État. Le floutage est basé sur l'analyse en composantes principales (ACP), et il est réversible, ce qui signifie que l'on peut récupérer la plaque désidentifiée en connaissant les coefficients de chaque composante principale.

2. Désidentification des identifiants biométriques physiologiques

2.1 visages dans les images fixes :

Le visage est une caractéristique biométrique essentielle dans les médias, et il doit être dépersonnalisé pour protéger la vie privée. Au départ, la dépersonnalisation des visages était appliquée aux images fixes en utilisant des méthodes comme la pixellisation ou le floutage pour cacher la zone du visage [26-27]. Cependant, pour une meilleure protection de la vie privée, des techniques plus avancées ont été développées. L'une d'entre elles remplace le visage original par un

visage reconstruit créé à partir de quelques visages de référence, perdant ainsi les détails du visage. Cependant, cela peut rendre les images dépersonnalisées peu naturelles.

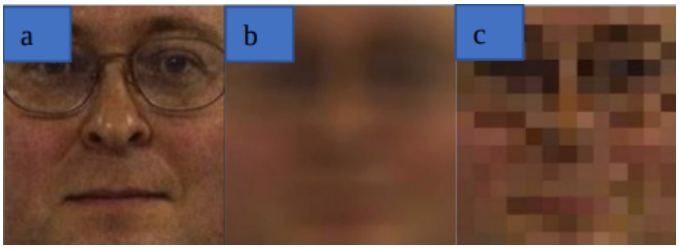


Figure II.1. Méthodes naïves de désidentification des visages : a) Image originale ; b) Flou : σ2= 18 ; c) Pixellisation : paramètre p = 12 [28].

D'autres méthodes, comme k-Same et ses variantes, ont été conçues pour équilibrer la protection de la vie privée et la qualité des images dépersonnalisées [29]. Celles-ci remplacent les visages par des visages anonymisés, ce qui garantit la confidentialité, mais peut introduire des distorsions indésirables.

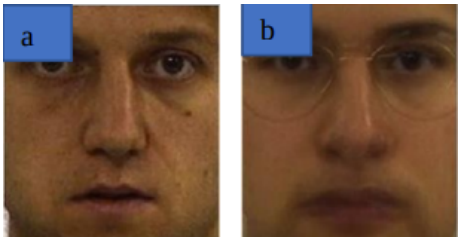


Figure II.2. Désidentification k-Same : a) image originale ; b) image désidentifiée pour k = 6 ; [28].

Enfin, des approches ont été développées pour la dépersonnalisation des photos en ligne. Ces méthodes préservent l'utilité des images tout en les rendant méconnaissables. Une méthode utilise la dé-identification naïve, tandis qu'une autre applique le brouillage des pixels [30].D'autres méthodes utilisent le morphing pour créer des visages méconnaissables tout en préservant la ressemblance. Le warping est une autre technique qui modifie les coordonnées faciales pour la dépersonnalisation[31]. Ces méthodes ont été testées sur des bases de données et ont montré des niveaux variables de naturalité et de protection de la vie privée.

2.2 Visages dans les systèmes de vidéosurveillance

Avec la prolifération des technologies visuelles, telles que les caméras de surveillance et les téléphones équipés d'appareils photo, la notion de "vie privée visuelle" est devenue importante. Elle englobe la collecte et la diffusion d'informations visuelles, les attentes en matière de vie privée du public, ainsi que les problèmes juridiques et éthiques qui en découlent. Une revue des méthodes de protection de la vie privée visuelle distingue cinq catégories principales [17] :

i) L'intervention : Empêcher la capture de données visuelles privées.
ii) La vision aveugle : Le traitement anonyme d'images ou de vidéos.
iii) Le traitement sécurisé : Le traitement respectueux de la vie privée des informations visuelles.
iv) La rédaction : Les méthodes basées sur la filtration d'images, le chiffrement, les algorithmes de type k-same, la suppression d'objets ou de personnes, et l'abstraction visuelle ou le remplacement d'objets.
v) La dissimulation de données : Les méthodes basées sur la stéganographie et le tatouage numérique.

La plupart de ces méthodes sont adaptées à la dépersonnalisation d'images fixes du visage prises de face ou à la télévision, mais ne conviennent pas aux systèmes de vidéosurveillance en raison de plusieurs raisons, notamment la dégradation de la qualité visuelle nécessaire à la sécurité, la perte du caractère naturel des images, les modifications irréversibles des vidéos et la nécessité de traiter en temps réel.

L'attention se tourne maintenant vers la protection de la vie privée dans les systèmes de vidéosurveillance, en particulier la dé-identification automatique des visages. Ce processus comprend la détection, le suivi et le masquage des visages[32]. Deux approches principales sont utilisées pour la détection des visages [33] : basée sur les caractéristiques et basée sur l'image. La première utilise des analyses visuelles de bas niveau, des caractéristiques faciales, et des modèles de forme active, tandis que la seconde repose sur des méthodes d'apprentissage.Le suivi facial est crucial pour préserver le caractère naturel des vidéos dé-identifiées, et il combine la détection des visages et leur suivi dans le temps. Le masquage est une méthode courante pour dé-identifier les visages, consistant à appliquer des filtres visuels. Le choix du filtre peut affecter les performances des algorithmes de reconnaissance faciale.

Une approche alternative est le brouillage des images du visage, utilisant des méthodes de transformation pour distordre l'image tout en restant réversible. Cela peut être fait en inversant pseudo-aléatoirement les coefficients de transformation ou en appliquant une permutation aléatoire[34-35]. Le brouillage est une option populaire dans le domaine de la vidéosurveillance.
L'efficacité de la détection, du suivi et de la dé-identification des visages est cruciale, car toute perte de détection entraîne une diminution significative de la protection de la vie privée.

2.3 Empreintes digitales

Au départ, l'idée de considérer les images fixes d'empreintes digitales comme des documents multimédias pourrait sembler étrange, principalement pour deux raisons. Premièrement, la reconnaissance d'empreintes digitales est souvent perçue comme une technologie biométrique bien connue, où les individus coopèrent en toute connaissance de cause.

Deuxièmement, notre principal intérêt concerne les documents multimédias collectés à distance. Cependant, deux facteurs importants ont motivé l'inclusion des empreintes digitales.[65]

En premier lieu, les systèmes biométriques basés sur les empreintes digitales dominent le marché biométrique, et avec leur expansion dans diverses applications de reconnaissance, la protection de la vie privée des empreintes digitales est devenue cruciale[36]. Deuxièmement, les recherches récentes indiquent qu'il est possible de détecter les empreintes digitales à distance en utilisant des techniques d'éclairage polarisé et des caméras spéciales, ce qui pourrait présenter des risques pour la vie privée à l'avenir[37].Il est à noter que les empreintes digitales contiennent non seulement des informations d'identification, mais aussi d'autres données sensibles, comme le sexe, l'origine ethnique, et même des informations médicales. Les méthodes traditionnelles de protection des empreintes digitales incluent des procédures telles que le flou, la pixellisation, la substitution par une empreinte digitale synthétique, ou l'application de filtres de confidentialité. Il est possible de réduire le risque d'identification en utilisant des empreintes digitales binaires dans le processus d'inscription, masquées par une clé d'incorporation de données[38].

Il existe également des méthodes basées sur la combinaison de deux empreintes digitales pour renforcer la protection de la vie privée. En utilisant ces méthodes, il est possible de convertir un modèle de points caractéristiques combiné en une image d'empreinte digitale synthétique, tout en préservant l'apparence réelle[39].

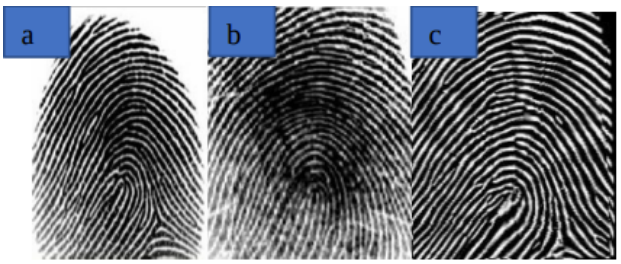


Figure II.3. Mélange d'empreintes digitales : a) empreinte originale ; b) fonction de transformation - empreinte d'un doigt différent ; c) nouvelle image d'empreinte digitale mélangée qui masque l'identité de l'empreinte originale [39].

D'autres méthodes visent à déformer les modèles biométriques originaux au niveau des caractéristiques pour masquer des informations sensibles comme le sexe ou l'origine ethnique. Une approche consiste à flouter l'image en utilisant une transformation des fréquences pour réduire la précision de l'estimation du sexe[40].

Cependant, à ce jour, il y a peu de recherches sur l'évaluation de la protection des informations médicales et d'autres données sensibles dans les empreintes digitales déformées de

cette manière, ainsi que sur leur impact sur les performances d'identification. Les études disponibles indiquent que les systèmes basés sur des empreintes digitales virtuelles combinées offrent des taux d'erreur relativement faibles en termes de faux rejets et de fausses acceptations.

2.4 L'iris

L'iris est une méthode importante pour identifier les personnes en utilisant des caractéristiques uniques de l'œil. Cela fonctionne bien pour l'identification car les caractéristiques entre différentes personnes sont très différentes, et elles restent constantes avec le temps. Cependant, la plupart des systèmes d'identification par l'iris nécessitent que les utilisateurs coopèrent en se rapprochant de la caméra, car l'iris est petit et nécessite une certaine résolution pour être capturé correctement. Cela signifie que les caméras doivent être relativement proches des personnes, généralement à une distance de 15 à 50 centimètres.

Il y a eu des progrès récents dans la technologie d'identification de l'iris qui permettent de capturer des images d'iris à plus longue distance sans que les sujets aient besoin de se rapprocher de la caméra. Par exemple, le système Iris at a Distance (IAD) peut identifier une personne à plus d'un mètre en moins d'une seconde[41].

Ces avancées posent des défis en matière de protection de la vie privée, car l'identification de l'iris à distance devient plus courante. De plus, de nombreux systèmes IAD capturent également des images du visage, ce qui signifie que la protection de la vie privée doit couvrir à la fois l'iris et le visage[42]. Cependant, il y a eu peu de recherches sur la protection de la vie privée de l'iris jusqu'à présent.

Une étude rare a abordé la dépersonnalisation de la région oculaire, y compris l'iris[43]. Ce système de dépersonnalisation utilise un module pour détecter automatiquement la région de l'œil et un module pour brouiller les images afin de protéger la vie privée. Les images brouillées empêchent la reconnaissance de l'iris et peuvent également affecter l'identification des visages en fonction de la taille des blocs de brouillage.

2.5 L'oreille

Bien que le visage et l'iris soient couramment utilisés pour identifier les personnes dans la biométrie, ils ont leurs problèmes[65]. La reconnaissance faciale peut échouer en raison de divers facteurs tels que les changements de posture, les expressions faciales, les barbes, les coiffures, les obstacles, le maquillage, le vieillissement et les variations d'éclairage dans des environnements non contrôlés. D'un autre côté, l'iris est stable, mais nécessite une caméra de haute résolution et un éclairage infrarouge proche pour être capturé à distance.C'est pourquoi l'oreille humaine est considérée comme une alternative pour l'identification des personnes à distance sans nécessiter leur coopération. Les systèmes de reconnaissance de l'oreille, qu'ils utilisent des images en 2D ou en 3D, ont montré des résultats prometteurs, même sans la coopération du sujet[44-45]. Ces

systèmes sont particulièrement utiles pour la surveillance intelligente.

Cependant, il y a encore des défis non résolus liés à la reconnaissance de l'oreille dans des situations réelles, comme les variations de pose, d'échelle, les conditions d'éclairage changeantes et les obstacles tels que les cheveux. Malgré des années de recherche, il n'y a actuellement aucun système commercial de reconnaissance de l'oreille, ce qui limite également les efforts de protection de la vie privée liés à l'oreille.

3. Système de sécurité

Ces dernières années, il y a eu un intérêt croissant pour les systèmes de protection de la vie privée en temps réel basés sur la vidéo. Par exemple, des systèmes comme Respectful Cameras, PrivacyCam, TrustCam, et De-Identification Camera ont été développés pour masquer les visages des personnes en temps réel.[65]

Le système Respectful Cameras suit des marqueurs colorés portés par les utilisateurs, comme des chapeaux ou des gilets, pour masquer les visages en utilisant un suivi basé sur un espace couleur 9D et un filtre de particules[46]. PrivacyCam utilise un processus de cryptage réversible appelé PICO pour masquer les régions d'intérêt, comme les visages, en brouillant les coefficients utilisés pour le codage d'image JPEG[47]. TrustCam est composé d'un réseau de caméras de confiance équipées de modules de plateforme de confiance (TPM) pour le chiffrement des données et protéger l'identité des personnes dans les vidéos[48]. La caméra de désidentification effectue une désidentification en temps réel en floutant les pixels dans une boîte englobante qui entoure les personnes détectées dans les vidéos[49].

Cependant, ces systèmes produisent des vidéos désidentifiées qui ne conservent pas le caractère naturel des vidéos originales. Pour obtenir une meilleure protection de la vie privée, certaines approches remplacent les visages par des visages génériques. Cela a été testé dans des vidéos pour améliorer le réalisme des vidéos désidentifiées. ces systèmes visent à protéger la vie privée des individus dans des vidéos en temps réel en masquant les visages ou en les remplaçant par des visages génériques, mais il reste des défis pour préserver l'apparence naturelle des vidéos tout en protégeant la vie privée.

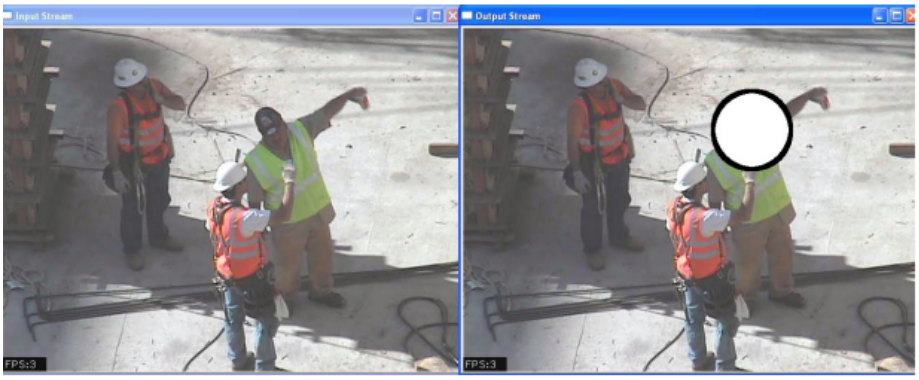


Figure II.4 Une image vidéo d'exemple est à gauche. Le résultat du système est affiché dans l'image de droite, où le visage de l'homme au gilet vert est masqué. Le reste de la scène, y compris les visages des travailleurs qui ne portent pas de gilets verts, reste visible[46]

4. Désidentification des identifiants biométriques comportementaux.

4.1. La démarche et des gestes

La démarche, soit la manière dont une personne marche, est une caractéristique comportementale unique qui peut être utilisée pour l'identification des individus[65]. Elle inclut des informations sur l'apparence physique, comme la silhouette, la taille et la forme des jambes, ainsi que des informations comportementales. Grâce aux avancées des systèmes de surveillance et de la vision par ordinateur, il est possible d'identifier des personnes en se basant sur leur démarche, même sans leur coopération.

Il existe deux approches principales pour la reconnaissance de la démarche : l'utilisation de capteurs tactiles portés par les individus, principalement pour des applications médicales, et l'analyse de vidéos pour capturer la démarche des personnes[50]. L'analyse vidéo peut être basée sur des modèles ou sur l'apparence[51]. Les approches basées sur des modèles identifient des paramètres spécifiques de la démarche et les comparent à des modèles préexistants, tandis que les approches sans modèle correspondent les images successives en se basant sur diverses caractéristiques telles que la position, la forme, la texture et la couleur.

La reconnaissance basée sur la silhouette est une approche courante pour la reconnaissance de la démarche. Cependant, la performance de ces systèmes varie en fonction de la qualité des séquences vidéo. Les technologies basées sur la démarche sont plus adaptées aux environnements contrôlés que pour une surveillance à grande échelle dans des espaces publics.La dé-identification de la démarche est un domaine de recherche encore peu exploré[52]. Certaines méthodes de flou et de déformation ont été proposées pour cacher l'information relative à la démarche dans les vidéos. Cependant, ces méthodes altèrent la naturalité des vidéos d'origine.

En ce qui concerne les gestes, ils représentent les mouvements du corps ou de parties du corps qui peuvent transmettre des informations ou être utilisés pour interagir avec l'environnement[53]. La variabilité des gestes peut également être exploitée pour l'identification des individus[54]. Bien que certaines recherches aient été menées pour développer des systèmes de vérification biométrique basés sur les gestes de la main, la dé-identification des gestes reste un domaine peu exploré, et des approches similaires à celles utilisées pour la démarche pourraient être appliquées pour résoudre ce problème.

5. Désidentification des identifiants biométriques souples

Les identifiants biométriques doux sont des caractéristiques physiques, comportementales ou humaines qui donnent des informations sur une personne mais ne sont pas suffisamment distinctifs ou permanents pour les différencier de manière fiable. Cependant, ces identifiants biométriques souples

peuvent être utilisés comme informations complémentaires pour améliorer la reconnaissance globale, surtout dans des scénarios moins stricts, tels que la reconnaissance à distance[55]. Il y a quatre principales manières d'utiliser ces identifiants biométriques souples :

i) Identifier ou vérifier une personne en se basant sur ces caractéristiques souples mesurées[55].

ii) Identifier ou vérifier une personne en utilisant des descriptions verbales de ces caractéristiques[57].

iii) Combiner ces identifiants biométriques souples avec des identifiants biométriques physiologiques ou comportementaux pour améliorer la précision de la reconnaissance[56].

iv) Extraire des informations des grandes bases de données biométriques[58-59].

Cependant, quel que soit le mode d'utilisation de ces identifiants biométriques doux, comme la silhouette, le sexe, la race, les grains de beauté, les tatouages, les taches de naissance et les cicatrices, ces informations portent atteinte à la vie privée des individus et doivent être dépersonnalisées dans les documents multimédias.

5.1 La silhouette du corps

La silhouette, qui correspond à la forme générale du corps, est un identifiant biométrique souple essentiel pour la reconnaissance des personnes. Elle peut être utilisée seule ou en combinaison avec d'autres identifiants biométriques, comme la démarche, pour identifier ou suivre les individus à travers différentes caméras dans les systèmes de surveillance.

Cependant, la dé-personnalisation de la silhouette est un domaine peu exploré. Dans certaines études, il a été montré que masquer une silhouette est relativement simple, que ce soit en agrandissant certaines parties du corps ou en appliquant un flou gaussien. Dans d'autres recherches, la meilleure méthode pour dé-personnaliser la silhouette a été identifiée en combinant la convolution intégrale de ligne (LIC) et un flou exponentiel des pixels[60].

Une approche pour la dé-personnalisation réversible des silhouettes dans les vidéos consiste à appliquer une distorsion à la région d'intérêt (ROI) contenant la silhouette en utilisant des méthodes de brouillage basées sur la transformation, telles que décrites dans certaines études. L'idée est de préserver la confidentialité tout en conservant la clarté de la vidéo.

Figure II.5 Résultat de la dépersonnalisation de la silhouette du corps par la méthode de brouillage[34].

5.2 Cicatrices, marques et tatouages

Les cicatrices, marques et tatouages (SMT) sont des caractéristiques corporelles qui peuvent être utilisées pour identifier une personne de manière plus précise que des éléments tels que l'âge, la taille, le genre et la race. Par exemple, des marques faciales comme les grains de beauté et les cicatrices ont été montrées comme améliorant la reconnaissance et la recherche automatique de visages[61].Cependant, il y a très peu d'études sur la dé-identification des cicatrices et des marques. En ce qui concerne les tatouages, ils sont de plus en plus courants, et environ 24% des adultes aux États-Unis en ont au moins un[62]. Ils sont principalement utilisés pour la recherche d'images basée sur le contenu, mais grâce à leurs caractéristiques visuelles et à leur emplacement sur le corps, ils peuvent également être utilisés pour identifier des individus ou des suspects dans le domaine de la criminalistique.

Pour la reconnaissance des tatouages, différentes méthodes telles que les caractéristiques de transformation invariante d'échelle (SIFT), les contours actifs et les caractéristiques "glocales" sont utilisées[63]. Malheureusement, il y a très peu de recherches sur la dé-identification des SMT, à l'exception d'une approche expérimentale qui visait à protéger la vie privée en localisant et en dé-identifiant les tatouages.

Figure II.6. Désidentification des tatouages ; a) Exemple d'une image fixe obtenue par un appareil photo couleur ; b) Caractéristiques SIFT extraites ; c) Image fixe de tatouage désidentifiée [64]

Dans cette méthode, la peau et les zones d'intérêt sont détectées, et les caractéristiques SIFT sont extraites pour comparer avec une base de données de modèles de tatouages. Les tatouages sont dé-identifiés en remplaçant la zone du tatouage par des pixels provenant de zones environnantes non tatouées, tout en essayant de conserver l'apparence naturelle de l'image dé-identifiée.

La recherche sur la dépersonnalisation des contenus multimédias est encore en cours malgré les efforts déployés par divers groupes[65]. Peu de progrès ont été réalisés en ce qui concerne la désidentification d'identifiants non biométriques, à l'exception des textes et des plaques d'immatriculation. Pour éviter l'identification forcée et la classification intrusive, nous devons faire plus d'efforts pour dépersonnaliser les styles vestimentaires et les coiffures.La dé-identification des plaques d'immatriculation reste un défi, en particulier dans les séquences vidéo. La protection de la vie privée dans les services web, comme Google Street View, est complexe car de nombreux visages ne sont pas floutés.La dé-identification des visages dans les images fixes est possible, mais des approches plus sophistiquées sont nécessaires pour maintenir la confidentialité et l'expression faciale. Dans les vidéos de surveillance, la détection des visages reste un défi, notamment dans des conditions difficiles.La dé-identification des empreintes digitales est complexe, tout comme la dé-identification de l'iris, de l'oreille, de la voix, de la démarche et des gestes. La protection de la vie privée dans le contenu multimédia reste un domaine de recherche en évolution.

CHAPITRE III :
Application et Résultat

Dans ce chapitre, nous abordons l'aspect pratique de notre système, en détaillant le choix du langage de programmation, de la plateforme et des outils que nous avons utilisés pour développer notre application.

1. Environnement de travaille :

L'environnement de travail se compose de deux éléments distincts, à savoir l'environnement matériel et l'environnement logiciel.

1.1 Environnement matériel :

Lenovo ThinkpadX280 :

Processeur : Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz.

Type de système : Windows 10 Professionnel 64 bits.

RAM : 8,00 GO.

Google Pixel 7:

Processeur : Google Tensor G2 Coprocesseur de sécurité Titan M2. RAM : 8 Go de RAM LPDDR5 128Go/256Go de stockage UFS3.110

1.2 Environnement Logiciel :

L'environnement logiciel est constitué de ce qui suit:

. Android Studio

. Flutter

2. Le langage utilisé pour le développement :

Nous avons implémenté notre application avec le langage de programmation :

Pour les raisons principales suivantes :

1. Syntaxe claire et expressive.
2. Compilé à la fois en code natif et en JavaScript.
3. Programmation réactive.
4. Framework Flutter.
5. Forte communauté et support.
6. Code partagé entre les plateformes .

Ces avantages font de Dart un langage attrayant pour le développement d'applications mobiles et web, offrant à la fois des performances élevées, une productivité accrue et une grande flexibilité.

3. Analyse et Conception de l'application

On va modéliser notre projet et ses unités utilisant le langage de modélisation unifié UML, et ensuite, on va créer l'application avec Flutter.

3.1 Diagramme de cas d'utilisation

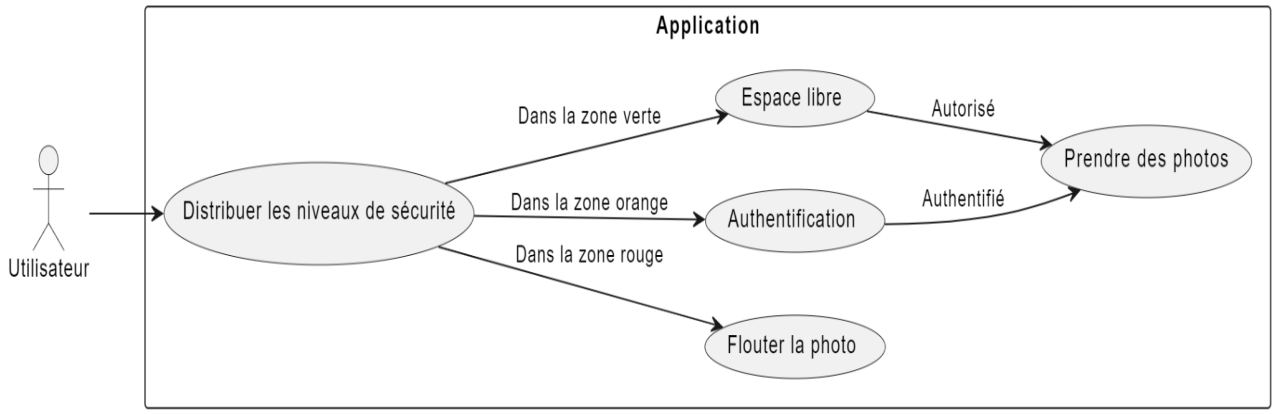


Figure III.1 Diagramme de cas d'utilisation

Ce diagramme présente les associations dans le cas ou l'utilisateur (un individu) veut prendre des photo et qu'il se trouve dans une des zone : vert, orange, rouge. Par exemple, si l'individu est dans une zone orange il doit d'abord passer par l'authentification, une fois vérifié, l'utilisateur peut prendre des photos. Il y a aussi le cas où il se trouve dans une rouge, l'application va directement flouter l'image prise et l'individu ne peut pas récupérer la photo originale. Enfin la zone verte ou l'utilisateur peut prendre des photos librement.

3.2 Diagramme de séquence

Nom : Gestion de la Sécurité en Fonction de la Position.

Description :

L'application vise à gérer les niveaux de sécurité en fonction de la position géographique de

l'individu, lui permettant de prendre des photos en respectant les règles de confidentialité et de sécurité

Scénario principal :

- L'utilisateur tente de prendre une photo.
- Le Système récupère les données de géolocalisation actuelles de l'utilisateur.
- Le Système détermine la zone en fonction des données de géolocalisation.
- Le Système applique les règles de sécurité appropriées en fonction de la zone.

Scénarios alternatifs :

- Si l'utilisateur ne s'authentifie pas avec succès dans la zone orange, il se voit refuser l'accès aux photos non floutées.

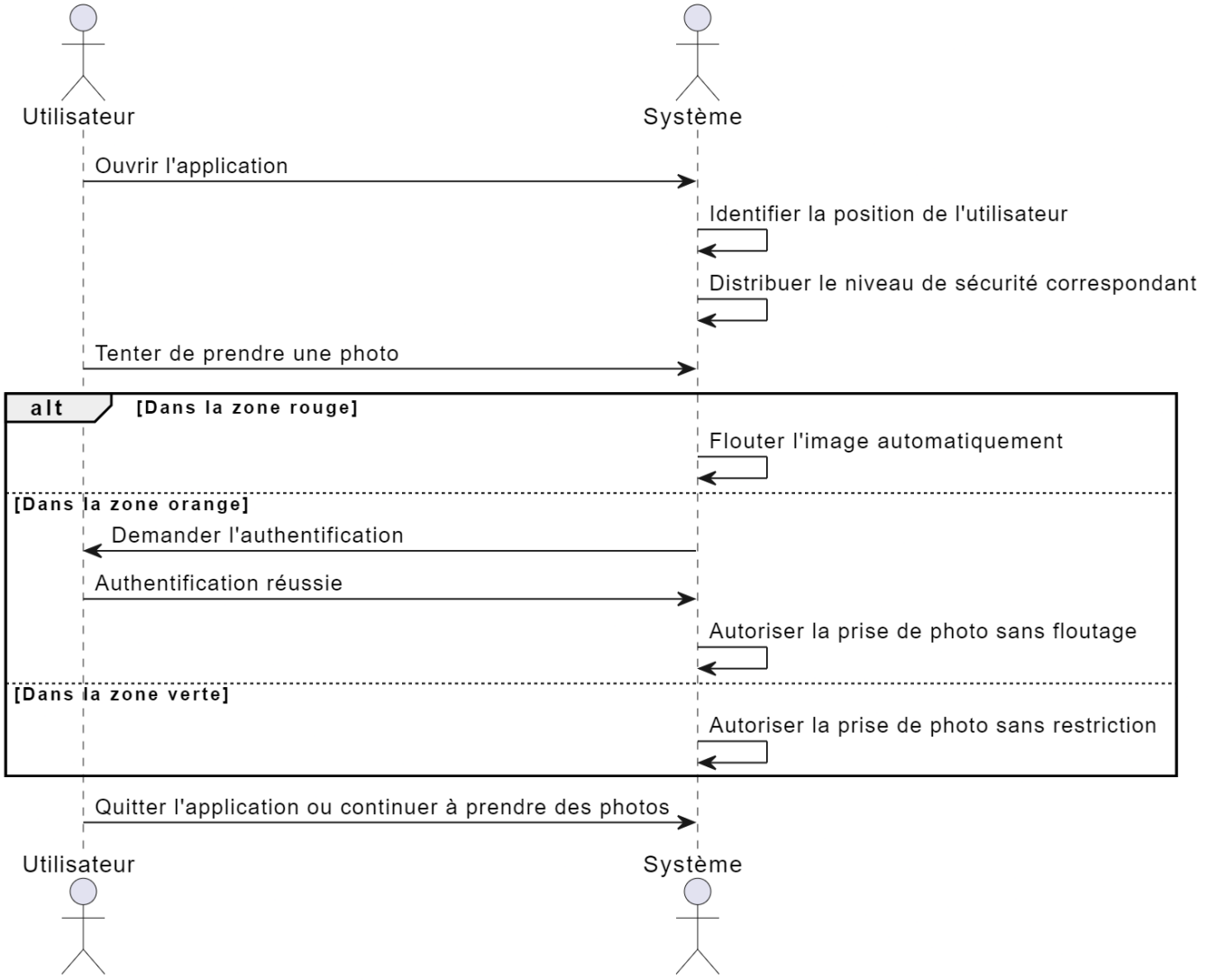


Figure III.2 Diagramme de séquence.

3.3 Création de l'application

Pour créer une application Flutter qui permet de prendre des photos avec un effet de flou d'arrière-plan, on a utilisé la bibliothèque caméra pour accéder à la caméra de l'appareil et la bibliothèque image pour appliquer l'effet de flou.

Voici les étapes pour créer cette application :

Ajoutez les dépendances nécessaires dans notre fichier pubspec.yaml :

```
camera: ^0.10.5+2
image: ^4.0.17
image_gallery_saver: ^2.0.3
```

Figure III.3.Dépendances pour caméra

Créez une page qui affiche la vue de la caméra et un bouton pour prendre la photo :

```
class ImagePreview extends StatefulWidget {
  final String imagePath;

  const ImagePreview({required this.imagePath, Key? key}) : super(key: key);

  @override
  _ImagePreviewState createState() => _ImagePreviewState();
}

class _ImagePreviewState extends State<ImagePreview> {
  late String blurredImagePath;
```

Figure III.4. Application Flutter de visualisation de la caméra en temps réel

```dart
@override
void initState() {
  super.initState();
  applyGaussianBlur();
```

Figure III.4. Application Flutter de visualisation de la caméra en temps réel

Dans la méthode applyBlur(), on a utilisé la bibliothèque image pour appliquer l'effet de flou à l'image.

Dans la méthode onPressed() du bouton, on prend la photo en utilisant controller.takePicture(), puis on applique l'effet de flou à l'image en utilisant la méthode applyBlur(). Enfin, on affiche l'image floue dans une nouvelle page en utilisant Navigator.push().

```dart
/ void applyGaussianBlur() {
  img.Image image = img.decodeImage(File(widget.imagePath).readAsBytesSync())!;
  img.Image blurredImage = img.gaussianBlur(image, radius: 100); // Niveau de flou gaussien prédéfini
  blurredImagePath = saveBlurredImage(blurredImage);
}*/

String saveBlurredImage(img.Image image) {
  Directory tempDir = Directory.systemTemp;
  String tempPath = tempDir.path;
  String blurredImagePath = '$tempPath/blurred_image.jpg';
  File(blurredImagePath).writeAsBytesSync(img.encodeJpg(image));
  return blurredImagePath;
}

void saveImage() async {
  final originalImage = File(widget.imagePath);
  final savedImage = File(blurredImagePath);
  final originalImageExists = await originalImage.exists();
  final savedImageExists = await savedImage.exists();

  if (originalImageExists && savedImageExists) {
    final result = await ImageGallerySaver.saveFile(savedImage.path);
    if (result['isSuccess']) {
      ScaffoldMessenger.of(context).showSnackBar(
        SnackBar(
          content: Text('Image saved to gallery'),
        ), // SnackBar
      );
    } else {
      ScaffoldMessenger.of(context).showSnackBar(
        SnackBar(
          content: Text('Failed to save image'),
        ), // SnackBar
```

Figure III.5. Traitement d'Image : Floutage en Flutter

La géolocalisation :

La conception de cette partie repose sur l'utilisation de la dépendance 'geolocator' pour obtenir la localisation de l'appareil.

```
geolocator: ^9.0.2
```

Figure III.6. Dépendance de la géolocalisation

Une fois la localisation obtenue, nous avons procédé à la création d'une carte en utilisant Google My maps.

Figure III.7. Une carte personnalisées dans google my maps Cette carte est ensuite intégrée à l'application avec la dépendance 'google_map_flutter' :

```
google_maps_flutter: ^2.4.0
```

L'objectif principal de cette approche est de vérifier si l'utilisateur se trouve actuellement dans une des zones en se basant sur les données de sa position géographique.

(a)

```
List<List<LatLng>> redPolygons = [
  // Liste des points pour le premier polygone rouge
  [LatLng(XX.XXXXX, YY.YYYYY), LatLng(XX.XXXXX, YY.YYYYY), ...],
  // Liste des points pour le deuxième polygone rouge
  ...
];

List<List<LatLng>> greenPolygons = [
  // Liste des points pour le premier polygone vert
  [LatLng(XX.XXXXX, YY.YYYYY), LatLng(XX.XXXXX, YY.YYYYY), ...],
  // Liste des points pour le deuxième polygone vert
  ...
];
```

```
bool isPositionInsidePolygon(List<LatLng> polygon, LatLng position) {
  int i, j = polygon.length - 1;
  bool isInside = false;
  for (i = 0; i < polygon.length; i++) {
    if ((polygon[i].latitude < position.latitude &&
        polygon[j].latitude >= position.latitude ||
        polygon[j].latitude < position.latitude &&
            polygon[i].latitude >= position.latitude) &&
        (polygon[i].longitude +
            (position.latitude - polygon[i].latitude) /
                (polygon[j].latitude - polygon[i].latitude) *
                (polygon[j].longitude - polygon[i].longitude) <
            position.longitude)) {
      isInside = !isInside;
    }
    j = i;
  }
  return isInside;
}
```

(b)

Figure III.8.(a) et (b) :Intégrer une Carte Google My Maps en Flutter

L’authentification :

Les dépendances nécessaires pour l’authentification sont :

```
firebase_core: ^2.14.0
firebase_auth: ^4.6.3
cloud_firestore: ^4.8.1
firebase_storage: ^11.2.3
```

Figure III.9.Dépendances pour l’authentification

```dart
class AuthentificationScreen extends StatefulWidget {
  final VoidCallback onAuthSuccess;

  AuthentificationScreen({required this.onAuthSuccess});

  @override
  _AuthentificationScreenState createState() => _AuthentificationScreenState();
}
class _AuthentificationScreenState extends State<AuthentificationScreen> {
  final TextEditingController emailController = TextEditingController();
  final TextEditingController passwordController = TextEditingController();
  Speciality selectedSpeciality = Speciality.Professeur;

  Future<void> _authenticate(String email, String password) async {
    FirebaseAuth auth = FirebaseAuth.instance;

    try {
      UserCredential userCredential = await auth.signInWithEmailAndPassword(
        email: email,
        password: password,
      );

      // Vérifiez si l'utilisateur existe dans la base de données Firestore
      User? user = userCredential.user;
      if (user != null) {
        // L'utilisateur existe dans la base de données Firestore
        widget.onAuthSuccess(); // Appeler la fonction de rappel
      } else {
        print('vous ne peuvez pas prendre une photo');
        // L'utilisateur n'existe pas dans la base de données Firestore
      }
    } catch (e) {
      // Une erreur s'est produite lors de l'authentification
```

Figure III.10.Vérification de l’authentification dans Flutter

4. Zone Rouge :

La page qui affiche la vue de la caméra et un bouton pour prendre la photo et un autre pour la rotation de la caméra :

Figure III.11. Caméra en temps réel avec prise de photo

La vérification en arrière plan la localisation :

Figure.III.7

L’affichage de l'image floue dans une nouvelle page :

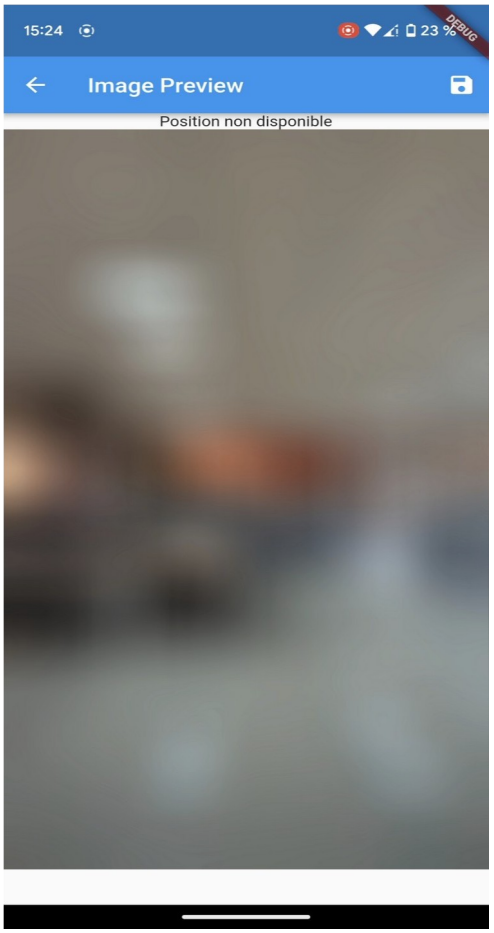


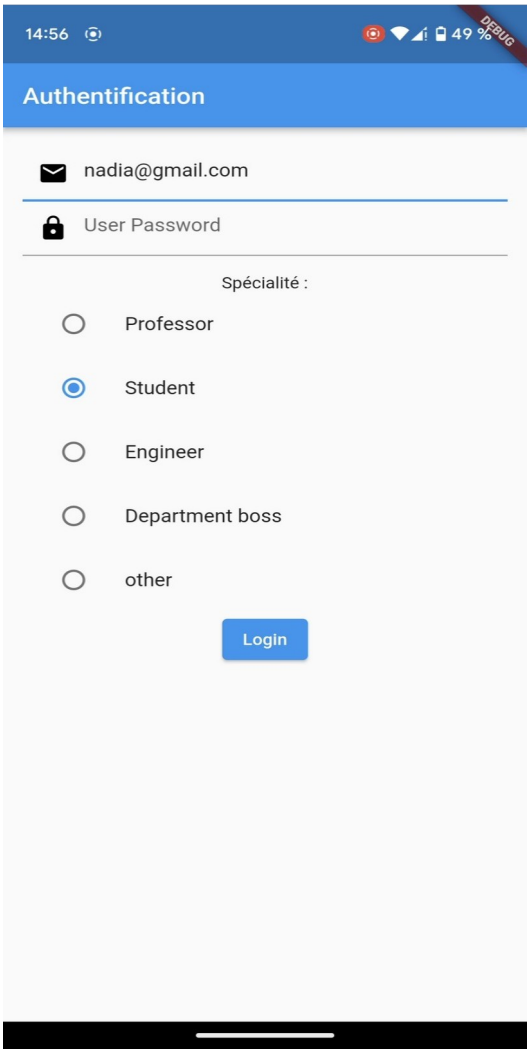
Figure III.12. Image flouté

L’utilisateur ne peut pas récupéré l’image originale car elle est flouté avant qu'elle ne soit enregistrée.

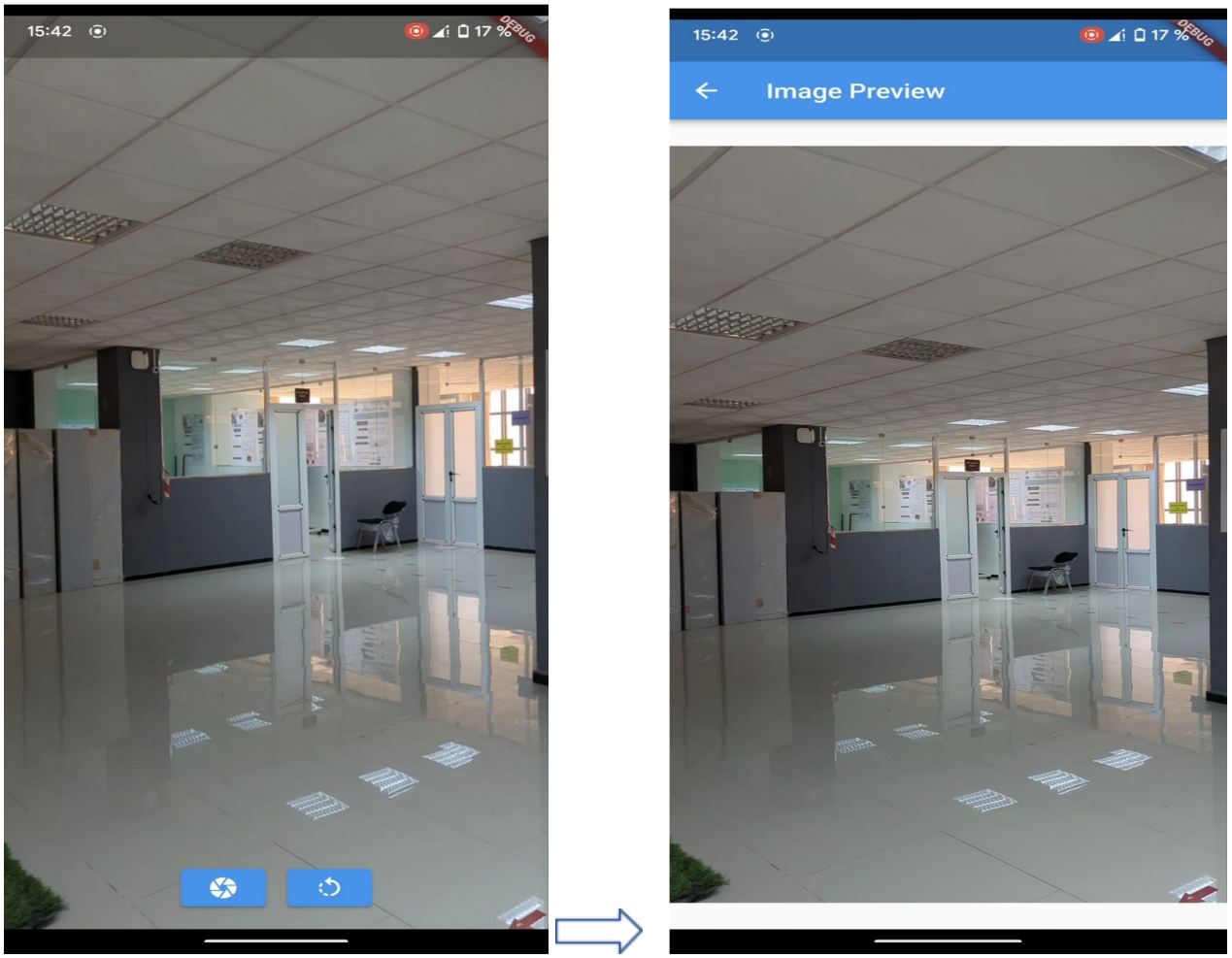
5. Zone orange :

Dans cette partie l'utilisateur doit d'abord faire une authentification, s'il existe dans la base de donnés alors il a le droit de prendre des photo, sinon il n'aura pas accès.

Figure III.13. Interface d'authentification



Une fois l'authentification est confirmée, l'utilisateur peut prendre des photos :

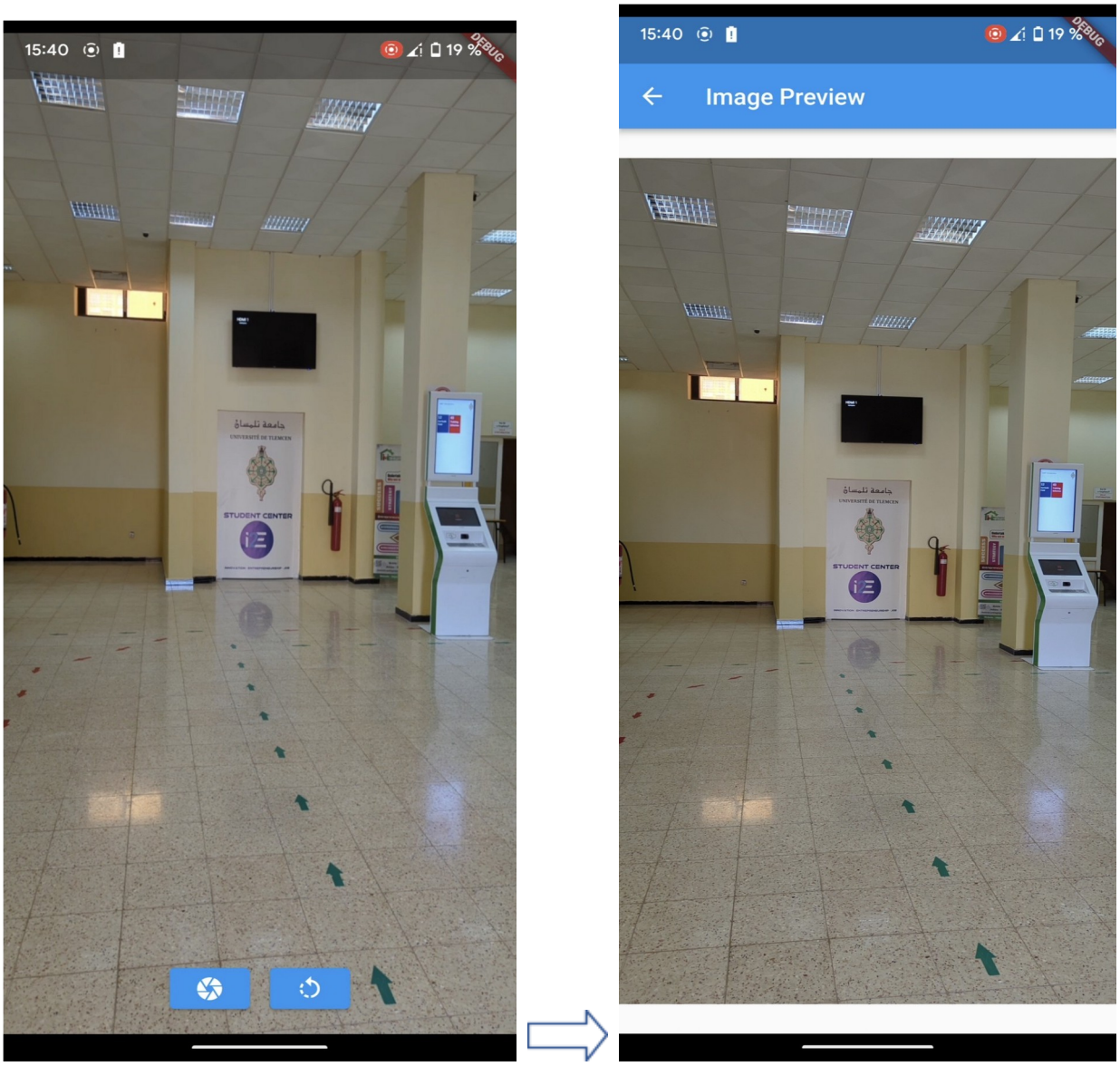


a)Caméra en temps réel avec prise de photo **b)** photo prise

6. Zone verte :

C’est la partie ou l’utilisateur peut prendre des photos tant qu’il est loin de les zones rouge et orange quelle que soit son identité.

Résultat :



(a) (b)

Figure III.14.a) Capture d'image en direct depuis la caméra ; **b)** Photo capturée.

7. Conclusion :

La protection contre les photos non autorisées est un enjeu important qui nécessite une solution efficace. Nous avons vu comment une application peut être utilisée pour localiser l'utilisateur et appliquer différents niveaux de protection en fonction de sa position géographique. Cette solution peut aider à prévenir les risques liés aux différentes méthodes d'attaque possibles et protéger la vie privée des individus.

Conclusion générale

Dans cette thèse, nous avons approfondi le domaine de la vie privée et de la désidentification, en nous concentrant sur les aspects techniques et conceptuels liés à la protection des données personnelles. Notre analyse est structurée en trois sections principales, dont chacune apporte une contribution significative à la compréhension et à la mise en œuvre du processus de suppression d'identification.

Le chapitre 1 a jeté les bases de notre recherche en exposant les principes de base en matière de confidentialité, en identifiant différents types de données sensibles et en présentant les théories clés. Nous avons également examiné les méthodes de protection de la vie privée, notamment la désidentification et une variation irréversible de cette méthode. Cette section a défini le cadre conceptuel essentiel pour la suite de notre travail. Dans chapitre 2, nous avons approfondi la suppression d'identité en explorant différentes techniques d'anonymisation des données, qu'il s'agisse d'identifiants biométriques non biométriques, de biométrie physiologique ou comportementale. Nous discutons également des systèmes de surveillance et de protection, en soulignant les défis spécifiques associés à la suppression d'identité dans ces contextes.

Le chapitre 3 nous permet de proposer une application pratique de nos connaissances. Nous avons conçu un environnement de travail pour mettre en œuvre efficacement la désidentification des données. Nous avons couvert des aspects tels que la sélection du langage de développement et la conception d'applications, fournissant ainsi une feuille de route pour mettre en pratique les concepts présentés précédemment. Enfin, nous avons présenté les résultats de la mise en œuvre de notre application. Cette phase pratique permet de confirmer la pertinence de nos méthodes de suppression d'identité et de démontrer leur efficacité en situation réelle. Les performances obtenues ont confirmé la faisabilité et la validité de notre méthode.

En conclusion, notre thèse couvre de manière exhaustive la confidentialité, la désidentification et l'application des lois. Nous avons couvert une variété de techniques et d'aspects, fournissant une base solide à quiconque cherche à protéger sa vie privée dans un monde de plus en plus axé sur la collecte et l'analyse de données. Notre proposition d'application offre un moyen concret de mettre en œuvre ces concepts, contribuant ainsi à protéger la vie privée dans divers contextes. Le défi actuel en matière de protection de la vie privée reste d'actualité et notre travail apporte une contribution précieuse à cette mission importante.

Pour une application

Business Model Canvas

PARTENAIRES

- Entreprise : Google/Apple
- Firebase
- Ministère de la défense

ACTIVITÉS CLÉS

- Technologie R&D
- Vente de notre service

RESSOURCES CLÉS

- Ordinateur
- Smartphone
- Cloud Firestore

PROPOSITION DE VALEUR

- Protection de la vie privé .
- Protection des zones sensible.
- Renforcer la sécurité

RELATION CLIENS

- Résaux Socieux
- Service clientèle

DISTRIBUTION

- En ligne.
- Android/ios

SEGEMENTS DE MARCHÉ

- Militaire
- Les hopiteaux
- Les industries
- Les usines
- Les établissement d'enseignement
- Les musés

STRUCTURE DE COUTS

- Smartphone Android/IOS
- 2030DA/mois Cloud
- 3380DA inscription une fois Google
- 13393DA/an inscription Apple

SOURCES DE REVENU ET MODELE DE PRICING

- 50000DA/mois vente de notre service plus 25000DA pour fonctionnalités supplémentaires

1. Proposition de Valeur :

Protection de la vie privée :
Notre application est conçue pour garantir une protection maximale de la vie privée de nos utilisateurs. En utilisant des protocoles de chiffrement de pointe, nous veillons à ce que les données personnelles des utilisateurs restent confidentielles, offrant ainsi une tranquillité d'esprit inégalée.

Protection des zones sensibles :
Notre technologie de pointe est spécialement adaptée pour sécuriser des zones sensibles. Les capteurs intégrés et les fonctionnalités de détection d'intrusion assurent un niveau de sécurité inégalé, que ce soit dans les bâtiments gouvernementaux, les installations militaires ou les zones industrielles à haute sécurité.

Renforcer la sécurité :
En fournissant un service fiable, notre application aide à renforcer la sécurité dans divers contextes. Des fonctionnalités telles que la surveillance en temps réel et les alertes personnalisables garantissent que nos utilisateurs sont toujours informés des menaces potentielles, ce qui leur permet de prendre des mesures préventives.

2. Segment de Marché :

Notre application a pour objectif de servir plusieurs segments de marché, notamment le militaire, les hôpitaux, les industries, les usines, les établissements d'enseignement et les musées. Chacun de ces secteurs a des besoins de sécurité spécifiques, et notre application est adaptée pour répondre à ces besoins de manière précise et efficace. Par exemple, dans le secteur médical, notre application est utilisée pour garantir la confidentialité des dossiers médicaux électroniques, tandis que dans le secteur militaire, elle assure la sécurité des bases militaires et des communications confidentielles.

3. Relation Client :

Réseaux Sociaux :
Nous utilisons activement les réseaux sociaux pour interagir avec nos clients et recueillir leurs commentaires. Notre présence en ligne permet aux utilisateurs de poser des questions, de partager leurs expériences et de rester informés des dernières mises à jour de l'application. Cela crée une communauté engagée et renforce la confiance des utilisateurs dans notre service.

Service clientèle :
Notre service clientèle dédié est une pierre angulaire de notre entreprise. Nos représentants du service clientèle sont disponibles 24 heures sur 24, 7 jours sur 7, pour

répondre aux questions et aux préoccupations des utilisateurs. Ils offrent un soutien personnalisé, résolvent les problèmes techniques et garantissent que chaque utilisateur a une expérience positive avec notre application.

4. Canaux de Distribution :

Nous distribuons notre application en ligne via les boutiques d'applications Google Play Store et Apple App Store. Cette stratégie de distribution nous permet de toucher un vaste public d'utilisateurs potentiels et de garantir un processus d'installation et de mise à jour facile et sécurisé pour nos clients.

5. Partenaires Clés :

Entreprise Google/Apple :
Notre partenariat stratégique avec Google et Apple est essentiel pour la distribution de notre application sur leurs plateformes respectives. Cette collaboration nous donne un accès instantané à des millions d'utilisateurs potentiels. Nous travaillons en étroite collaboration avec ces géants de la technologie pour optimiser la visibilité de notre application et garantir une expérience utilisateur optimale.

Firebase :
Firebase est notre partenaire technologique de confiance. Ils fournissent des services essentiels de développement et de gestion de l'application, ce qui nous permet de maintenir un haut niveau de qualité et de fiabilité pour nos utilisateurs.

Ministère de la Défense :
Notre partenariat avec le Ministère de la Défense renforce considérablement notre crédibilité dans le secteur de la sécurité. Cela nous permet de cibler un marché spécifique en fournissant des solutions sur mesure pour répondre à leurs besoins uniques.

6. Activités Clés :

Technologie R&D :
Une part essentielle de nos activités consiste en la recherche et le développement (R&D) pour améliorer en permanence notre application. Nous investissons dans la R&D pour renforcer la sécurité, améliorer les fonctionnalités de protection de la vie privée et garantir que notre application reste à la pointe de la technologie. Notre équipe de chercheurs travaille sur l'innovation en matière de cybersécurité et de surveillance pour maintenir notre leadership dans le secteur.

Vente de notre service :

Notre activité principale consiste à vendre notre application aux utilisateurs finaux. Cela inclut la gestion des canaux de vente, la tarification, la négociation de contrats et la prestation de services aux clients.

7. Ressources Clés :

Ordinateur :
Les ordinateurs sont essentiels pour le développement, la gestion et l'amélioration continue de notre application. Notre équipe de développement dépend de ces ressources pour créer, tester et déployer des mises à jour et des améliorations.

Smartphone :
Les smartphones sont la principale plateforme utilisée par nos clients finaux pour accéder à notre application. Nous devons garantir la compatibilité avec un large éventail de dispositifs, ce qui nécessite des ressources pour le développement, les tests et le support.

Cloud Firestore :
Pour stocker et gérer les données sensibles de nos utilisateurs, nous faisons appel à des services de stockage en nuage comme Cloud Firestore. Cela nécessite une infrastructure de serveurs robuste et des compétences pour gérer efficacement ces ressources.

8. Structure de Coûts :

Smartphone Android/iOS :
Nous investissons considérablement dans le développement et la maintenance de notre application sur les plateformes Android et iOS. Cela englobe les coûts liés au développement de fonctionnalités spécifiques à chaque plateforme, ainsi que les mises à jour régulières pour rester compatibles avec les nouvelles versions des systèmes d'exploitation.

Cloud :
Les coûts mensuels liés à l'utilisation du Cloud Firestore comprennent l'hébergement des données, la bande passante et la sécurité. Nous devons surveiller de près ces coûts pour garantir une utilisation efficace des ressources cloud.

Inscription Google/Apple :
Pour distribuer notre application sur Google Play Store et Apple App Store, nous devons payer des frais d'inscription uniques sur ces plateformes de distribution. Cela fait partie de nos coûts initiaux pour mettre notre application à la disposition du public.

9. Source de Revenus et Modèle de Prix :

Nous générons des revenus principalement en vendant notre service principal aux utilisateurs. Le modèle de prix est basé sur un abonnement mensuel de 50000 DA par utilisateur, garantissant un flux de revenus régulier et prévisible.En outre, nous proposons des fonctionnalités supplémentaires à nos clients moyennant des frais supplémentaires de 25 000 DA chacune. Ces fonctionnalités incluent des services premium, des mises à jour personnalisées et un support avancé. Ce modèle de tarification flexible nous permet de répondre aux besoins variés de notre clientèle et d'augmenter nos revenus grâce à des offres personnalisées.

Bibliographie

[1] plato, http://plato.stanford.edu, (2009) (accessed 12.06.14).

[2] S. D. Warren, L. D. Brandeis, The Right to Privacy, Harvard Law Review, vol. IV, no. 5. (1890) http://readingnewengland.org/app/books/righttoprivacy/ (accessed 02.06. 14).

[3] A. F. Westin, Social and Political Dimensions of Privacy, The Society for the Psychological Study of Social Issues, (2003) 431 - 453.

[4] D. J. Solove, Understanding Privacy, Harvard University Press, Cambridge, 2008.

[5] P. Campisi, Security and Privacy in Biometrics: Towards a Holistic Approach, in: P. Campisi (Ed.), Privacy and Security in Biometrics, Springer, 2013, pp. 1 – 24.

[6] S. Rane, Standardization of Biometric Template Protection, IEEE MultiMedia, vol. 21, no. 4, (2014) 94 - 99.

[7] C. Rathgeb, A. Uhl, A Survey on Biometric Cryptosystems and Cancelable Biometrics, EURASIP Journal on Information Security 2011:3, (2011) 1 - 25. http://jis.eurasipjournals.com/content/2011/1/3 (accessed 10.01.15)

[8] V. M. Patel, N. K. Ratha, R. Chellappa, Cancelable Biometrics: A Review, IEEE Signal Processing Magazine, vol. 32, no. 5, (2015) 54 - 65.

[9] T. E. Boult, PICO: Privacy through Invertible Cryptographic Obscuration, IEEE/NSF Proc. of the Workshop on Computer Vision for Interactive and Intelligent Environments, (2005) 27 - 38.

[10] A. J. Bharucha, A. J. London, D. Barnard, H. Wactlar, M. A. Dew, C. F. Reynolds III, Ethical Considerations in the Conduct of Electronic Surveillance Research, Journal of Law, Medicine & Ethics, (2006) 1 - 10.

[11] Common Criteria for Information Technology Security Evaluation, (1999). https://www.niap-ccevs.org/Documents_and_Guidance/cc_docs/cc_users_guide.pdf (accessed 08.07.13).

[12] G. W. van Blarkom, J. J. Borking, J. G. E. Olk, (Eds.), Handbook of Privacy and PrivacyEnhancing Technologies, College Bescherming Persoonsgegevens, The Hague, 2003.

[13] P. Langendörfer, M. Maaser, K. Piotrowski, S. Peter, Privacy Enhancing Techniques: A Survey and Classification, (2008) 1 - 18. http://www.ics.uci.edu/~steffenp/files/langendoerfer2008privacy.pdf (accessed 29.11.15).

[14] A. Cavoukian, Privacy by Design, (2010) 1 - 2. https://www.privacybydesign.ca (accessed 07.11.15).

[15] G. S. Nelson, Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification, (2015) 1 - 23. http://thotwave.com/wp-content/uploads/2015/09/data_sharing_privacy_anonymization_and_deide ntification_rev_13.pdf (accessed 25.06. 15).

[16] IC1206 COST Action, Memorandum of Understanding (MoU) (2013) http://w3.cost.eu/fileadmin/domain_files/ICT/Action_IC1206/mou/IC1206-e.pdf (accessed 03.12.15).

[17] J. R. Padilla-Lopez, A. A. Chaaraoui, F. Florez-Revuelta, Visual Privacy Protection Methods: A Survey, Expert Systems with Applications, 42 (9) (2015) 4177 - 4195.

[18] V. Bhagwan, T. Grandison, C. Maltzahn, Recommendation-based De-Identification, A Practical Systems Approach Towards De-identification of Unstructured Text in Healthcare, (2012) 155 - 162. http://www.almaden.ibm.com/cs/people/tgrandison/SPE2012-ReDid.pdf (accessed 15.07.14).

[19] I. Neamatullah, M. M. Douglass, L. H. Lehman, A. Reisner, M. Viallarroel, W.J. Long, et al., Automated De-identification of Free-text Medical Records, BMC Medical Informatics and Decision Making, vol. 8, no. 32 (2008) 1 – 73

[20] R. Fraser, D. Willison, Tools for De-Identification of Personal Health Information, Canada Health Infoway, (2009) 1 - 40. http://www.ehealthinformation.ca/wp-content/uploads/2014/08/deid.pdf (accessed 05.05.16).

[21] L. S. Garfinkel, NISTIR 8053 De-Identification of Personal Information, (2015) 1 - 54. http://dx.doi.org/10.6028/NIST.IR.8053 (accessed 17.12.15).

[22] D. Chen, Y. Chang, R. Yan, J. Yang, Protecting Personal Identification in Video, in: A. Senior (Ed.), Protecting Privacy in Video Surveillance, Springer, Dordrecht, 2009, pp. 115 – 128.

[23] P. Agrawal, De-identification for Privacy Protection in Surveillance Videos, Master of Science Thesis, Center for Visual Information Technology International Institute of Information Technology Hyderabad, (2010) 49 pages.

[24] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Neven, L.Vincent, Large-scale Privacy Protection in Google Street View, Proc. of the IEEE 12th Int. Conf. on Computer Vision (ICCV), (2009) 2373 - 2380.

[25] L. Du, H. Ling, Preservative License Plate De-identification for Privacy Protection, Proc. of the Int. Conf. on Document Analysis and Recognition (ICDAR), (2011) 468 - 472.

[26] M. Boyle, C. Edwards, S. Greenberg, The Effects of Filtered Video on Awareness and Privacy, Proc. of the ACM Conf. on Computer Supported Cooperative Work, Philadelphia, (2000) 1 – 10.

[27] C. Neustaedter, S. Greenberg, M. Boyle, Blur Filtration Fails to Preserve Privacy for Home - Based Video Conferencing, ACM Trans. on Computer Human Interaction, vol. 13, issue 1, (2006) 1 – 36.

[28] S. Ribaric, N. Pavesic, An Overview of Face De-identification in Still Images and Videos, Proc. of the 11th IEEE Int. Conf. and Workshops on Automatic Face and Gesture Recognition (FG), (2015) 1 - 6.

[29] E. Newton, L. Sweeney, B. Malin, Preserving Privacy by De-identifying Facial Images, IEEE Trans. on Knowledge and Data Engineering, vol. 17, no. 2, (2005) 232 – 243.

[30] R. Gross, L. Sweeney, F. de la Torre, S. Baker, Model-Based Face De-Identification, Proc. of the Conf. on Computer Vision and Pattern Recognition Workshop (CVPRW), (2006) 161 – 169.

[31] P. Korshunov, T. Ebrahimi, Using Face Morphing to Protect Privacy, Proc. of the IEEE Int. Conf. on Advanced Video and Signal-based Surveillance, (2013) 208 – 213.

[32] A. Senior, Privacy Protection in a Video Surveillance System, in: A. Senior (Ed.), Protecting Privacy in Video Surveillance, Springer, Dordrecht, 2009, pp. 35 - 47.

[33] E. Hjelmas, B. K. Low, Face Detection: A Survey, Computer Vision and Image Understanding 83, (2001) 236 – 274.

[34] F. Dufaux, T. Ebrahimi, Scrambling for Privacy Protection in Video Surveillance Systems, IEEE Trans. on Circuits and Systems for Video Technology, vol. 18, no. 8, (2008) 1168 – 1174.

[35] F. Dufaux, T. Ebrahimi, A Framework for the Validation of Privacy Protection Solutions in Video Surveillance, Proc. of the IEEE Int. Conf. on Multimedia and Expo (ICME), (2010) 66 - 71.

[36] MarketsandMarkets, Next Generation Biometric Market-Forecasts & Analysis 2014 - 2020, (2014), www.marketsandmarkets.com (accessed 15.11.15).

[37]technologyreview,(2015)https://www.technologyreview.com/s/422400/fingerprints-go-th edistance (accessed 07.12.15).

[38] L. Sheng, A. C. Kot, Fingerprint Combination for Privacy Protection, IEEE Trans. on Information Forensics and Security, vol. 8, no. 2, (2013) 350 – 360.

[39] A. Ross, De-identifying Biometric Images for Enhancing Privacy and Security, (2014) 1 - 27. http://biometrics.nist.gov/cs.../08_tuesday_ross_VC-MIXING_IBPC2014.pdf (accessed 17.12.15).

[40] L. Lugini, E. Marasco, B., Cukic, J. Dawson, Removing Gender Signature from Fingerprints, Proc. of the Special Session on Biometrics, Forensics, De-identifications and Privacy Protection (BiForD), (2014) 63 - 67

[41]morpho(2014).http://www.morpho.com/en/media/20140311_iris-distance-power-behind-iris (accessed 23.07.14).

[42] J. A. De Villar, R. W. Ives, J. R. Matey, Design and Implementation of a Long Range Iris Recognition System, Proc. of the Conf. Record of the 44th Asilomar Conf. on Signals, Systems and Computers (ASILOMAR), (2010) 1770 - 1773.

[43] D. Lee, K. N. Plataniotis, A Novel Eye Region Based Privacy Protection Scheme, Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), (2012) 1845 - 1848.

[44] A. Abaza, A. Ross, C. Hebert, M. A. F. Harrison, M. S. Nixon, A Survey on Ear Biometrics, ACM Comput. Surv. 45, 2, Article 22, (2013) 1 - 35.

[45] A. Pflug, C. Busch, Ear Biometrics: A Survey of Detection, Feature Extraction and Recognition Methods, IET Biometrics, vol. 1, issue 2, (2012) 114 - 129.

[46] J. Schiff, M. Meingast, D. K. Mulligan, S. Sastry, K. Goldberg, Respectful Cameras: Detecting Visual Markers in Real-time to Address Privacy Concerns, in: A. Senior (Ed.), Protecting Privacy in Video Surveillance, Springer, Dordrecht, 2009, pp. 65 – 89.

[47] A. Chattopadhyay, T.E. Boult, PrivacyCam: a Privacy Preserving Camera Using uCLinux on the Blackfin DSP, Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), (2007) 1 – 8.

[48] T. Winkler, B. Rinner, TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera based on Trusted Computing, Proc. of the 7th IEEE Int. Conf. on Advanced Video and Signal Based Surveillance (AVSS), (2010) 593 - 600.

[49] M. Mrityunjay, P. J. Narayanan, The De-Identification Camera, Proc. of the 3rd National Conf. on Computer Vision, Pattern Recognition, Image Processing and Graphics, (2011) 192 - 195.

[50] Z. Zhang, M. Hu, Y. Wang, A Survey of Advances in Biometric Gait Recognition, CCBR 2011, Lecture Notes in Computer Science (LNCS), vol. 7098, Springer, 2011, pp. 150 - 158.

[51] N. V. Boulgouris, D. Hatzinakos, K. N. Plataniotis, Gait Recognition: A Challenging Signal Processing Technology for Biometric Identification, IEEE Signal Processing Magazine, vol. 11, (2005) 78 – 90.

[52] N. Baaziz, N. Lolo, O. Padilla, F. Petngang, Security and Privacy Protection for Automated Video Surveillance, Proc. of the IEEE Int. Symposium on Signal Processing and Information Technology, (2007) 17 - 22.

[53] N.D. Lentsoane, K. Kith, B.J. Van Wyk, M. A. Van Wyk, Identity Verification System Using Hand Gesture Information, Proc. of the 17th Int. Symposium of the Pattern Recognition Society of South Africa, (2006) 1 - 6. http://www.prasa.org/proceedings/2006/prasa06-13.pdf (accessed 12.04. 16).

[54] S. Sclaroff, M. Betke, G. Kollios, Alon, Jonathan, V. Athitsos, Rui Li, J. Magee, Tai-Peng Tian, Tracking, Analysis, and Recognition of Human Gestures in Video, Proc. of the 8th Int. Conf. on Document Analysis and Recognition (ICDAR), vol.2, (2005) 806 – 810.

[55] P. Tome, J. Fierrez, R. Vera-Rodriguez, M. S. Nixon, Soft Biometrics and Their Application in Person Recognition at a Distance, IEEE Trans. on Information Forensics and Security, vol. 9, no. 1, (2014) 464 – 475.

[56] A. K. Jain, S. C. Dass, K. Nandakumar, Soft Biometric Traits for Personal Recognition Systems, Proc. of the Int. Conf. on Biometric Authentication, (2004) 731 – 738.

[57] D. A. Reid, M. S. Nixon S. V. Stevenage, Soft Biometrics; Human Identification Using Comparative Descriptors, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 36, no. 6, (2014) 1216 - 1228.

[58] J. L. Waymann, Large-scale Civilian Biometric Systems Issues and Feasibility, Proc. of the Card Tech / Secur. Tech ID, (1997).

[59] U. Park, A. K. Jain, Face Matching and Retrieval Using Soft Biometrics, IEEE Trans. on Information Forensics and Security, vol. 5, no. 3, (2010) 406 - 415.

[60] P. Agrawal, P. J. Narayanan, Person De-Identification in Videos, IEEE Trans. on Circuits and Systems for Video Technology, vol. 21, no. 3, (2011) 299 - 310.

[61] A. K. Jain, U. Park, Facial Marks: Soft Biometric for Face Recognition, Proc. of the 16th IEEE Int. Conf. on Image Processing (ICIP), (2009) 37 - 40.

[62] A. E. Laumann, A. J. Derick, Tattoos and Body Piercing in the United States: A National Dataset, of the American Academy of Dermatology, vol. 55, issue 3, (2006) 413 – 421.

[63] S. T. Acton, A. Rossi, Matching and Retrieval of Tattoo Images: Active Contour CBIR and Glocal Image Features, Proc. of the IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), (2008) 21 – 24.

[64] D. Marcetic, S. Ribaric, V. Struc, N. Pavesic, An Experimental Tattoo Deidentification System for Privacy Protection in Still Images, Proc. of the Special Session on Biometrics, Forensics, Deidentification and Privacy Protection (BiForD), (2014) 57 - 62.

[65] Ribaric, S., Ariyaeeinia, A., & Pavesic, N. (2016). De-identification for privacy protection in multimedia content: A survey. Signal Processing: Image Communication, 47, 131–151.