Invasion privée à cause de la vision par ordinateur

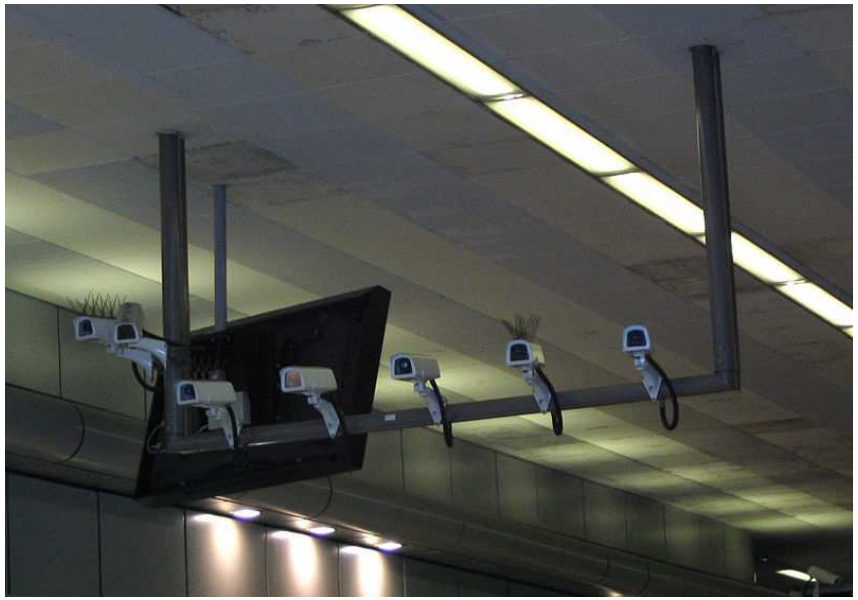
Auteurs: *Andrew Senior, Sharath Pankanti, Arun Hampapur, Lisa Brown, Ying-Li Tian, Ahmet Ekin, Jonathan Connell, Chiao Fe Shu et Max Lu - IBM T.J. Watson Research Center*

Présentée par : Quoc Anh LE

Avant-propos

- De plus en plus, la vidéosurveillance est largement utilisée dans les lieux publics et privés pour surveiller les allers et venus, prévenir les vols, agressions, fraudes et gérer les incidents et mouvements de foule. (*grâce au développement de la technologie, la réduction du coût des caméra de surveillance et des matériels de stockages numériques*)

- Informations humaines extraites de façon plus intelligente grâce aux algorithmes de la vision par ordinateur (l'identification des visages, le comportement bizarre, etc.)



Problématique

- L'abus des données obtenues par la vidéosurveillance (Selon une enquête de l'Angleterre, certaines opérateurs utilisent les vidéosurveillances pour le but de voyeurisme plutôt que la surveillance protectrice)
- Les images privées ne sont pas protégées.
- L'accès et l'exploitation des données lors de la transmission

Introduction

- Les auteurs ont proposé un système de sécurité (de façon de minimiser l'invasion privée)
  - Protéger les données lors de la transmission
  - Supprimer les informations privées des données enregistrées

Le système de la vidéosurveillance automatique.

- Indexer et enregistrer les signaux vidéos automatiquement
- Analyse des comportement d'une personne, les mouvements d'une personne par plusieurs caméras afin de comprendre leur interaction et leur intention.
- Reconnaissance des visages

Informations privées

- Distinction ambiguë
- Les images obtenues par les vidéosurveillances placées sur les rues publics ne sont pas privées et donc elles ne seront pas protégées. Mais avec la capacité du zoom, du ralenti, de la vision de nuit, du traitement d'image,… on peut exploiter plus informations ce qu'on regarde dans la rue.
- Proposition:
  - Confier toutes les contrôles aux opérateurs comme aujourd'hui
  - Construire un filtre adaptable (qui peut voir quelle information)

Les types des vidéosurveillances

- Anonymes: Le système sans ordinateur, c'est-à-dire que sans le traitement
- ID absolue: Le système peut identifier un individu (grâce à la technologie de reconnaissance des visage par exemple) et le relie à une personne dans la base des données.
- ID relative: Le système peut reconnaître une personne qu'il a déjà vu pendant une journée pour faire une statistique (le nombre des arrivées et des sorties) mais il n'a pas besoin d'identifier cette personne

Modèle du système proposé (1-2)

1. Quelle donnée est présentée?
   - Limitation de la vue du système aux zones uniques nécessaires et non privées.
   - Restreins les individus identifiés qui vont être présentés.
2. Est-ce que les sujets observés sont d'accord?
   - Si oui, le problème privé est laissé passer (
   - Mais certaines gens ne comprennent pas bien la protection privée. Et il est difficile d'obtenir tout accord dans un lieu public (normalement, on informe au publique qu'ils sont observés par les vidéosurveillances, mais ce n'est pas à dire que tout le monde est d'accord)
   - Dans le futur, les personnes peuvent accéder au système pour vérifier les données correspondantes à eux (ils peuvent supprimer ces informations comme **les « CNIL » européennes précisent les règles applicables aux moteurs de recherche**.)

Modèle du système proposé (3-4)

3. Quelle forme des données sont pris?
   - Les données enregistrées peuvent être supprimées?
   - Elles sont enregistrées lors de la transmission par un réseau?
   - Sont-elles chiffrées? Sont-elles accessibles à une seule personne ou il a besoin plusieurs clés pour les déchiffrer.
   - Chiffre des données assure que les espions ne peuvent pas exploiter les données enregistrées or les données en cours de la transmission (alors, les caméras chiffrent les données eux-mêmes).
4. Qui voit les images?
   - Les données sont limitées au police? aux sécurité professionnelles? Comment peut-on protéger contre les pirates?
   - En utilisant les clés différentes, chaque utilisateur peut voir une partie des données possibles (en divisant en plusieurs niveaux de sécurité selon les fonctions (recherche, ralenti,..) ou les parties de données).

Modèle du système proposé (3-4)

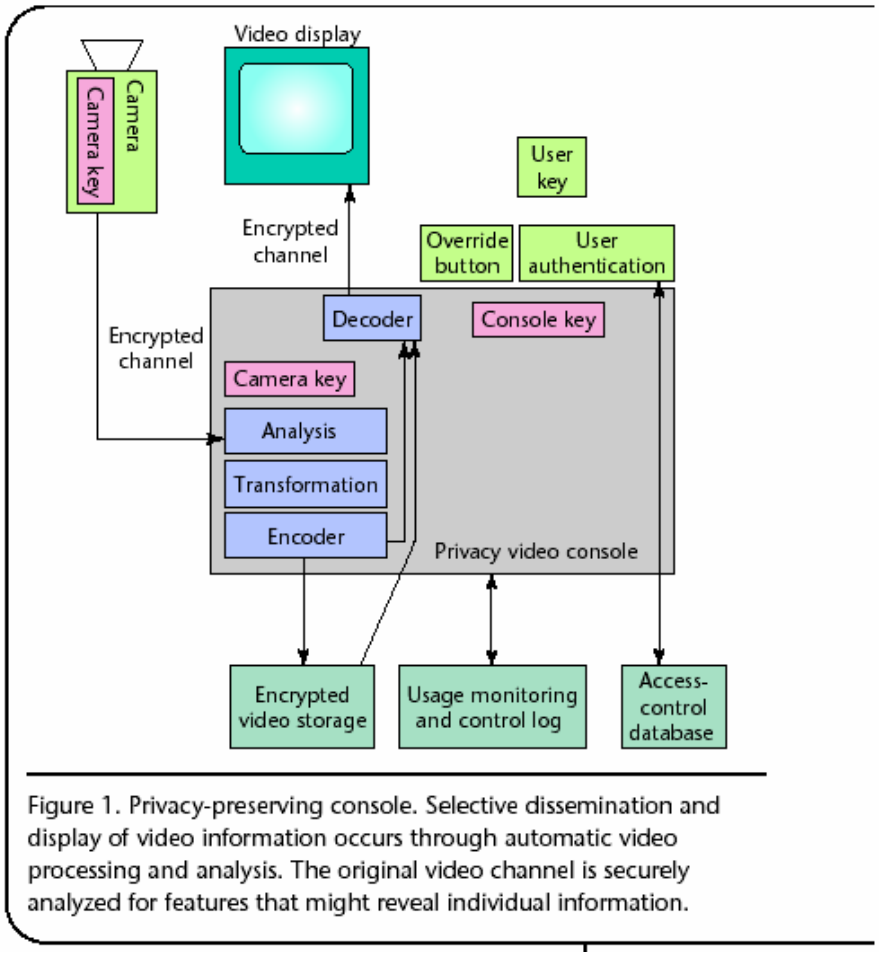


Figure 1. Privacy-preserving console. Selective dissemination and display of video information occurs through automatic video processing and analysis. The original video channel is securely analyzed for features that might reveal individual information.

Modèle du système proposé (5-6)

5. Combien de temps les données sont-elles stockées?
   - Non seulement la taille des données est limitée mais on doit aussi limiter le nombre qui peuvent les voir.
   - En utilisant les clés expirées pour définir le temps de la vie des données

6. How raw is the data?
   - On peut insérer les informations de temps ou les autres méta données aux vidéos pour plus accessible
   - A video-processing system could mask privacy-invasive features, to prevent it from being processed to extract metadata

Législation de la protection de vidéo privé

- DPA (Data Protection Act) in 1998 in UK, la législation se compose:
  - Traitement légal et honnête (fairly)
  - But limité
  - Adéquat, utile et pas excessif
  - Juste ou précis
  - Pas stocké plus le temps nécessaire
  - Conformément à la loi d'accès
  - Sécurité
  - Non transmis sans protection adéquate

Modèle du contrôle d'accès des données

Il y a trois couches:

1. Les utilisateurs ordinaires peuvent voir les informations statistiques des vidéos
2. Les utilisateurs privilégies peuvent voir certaines informations privées limitées
3. Les utilisateurs exécutifs légaux peuvent voir toutes les informations concernant chaque individu

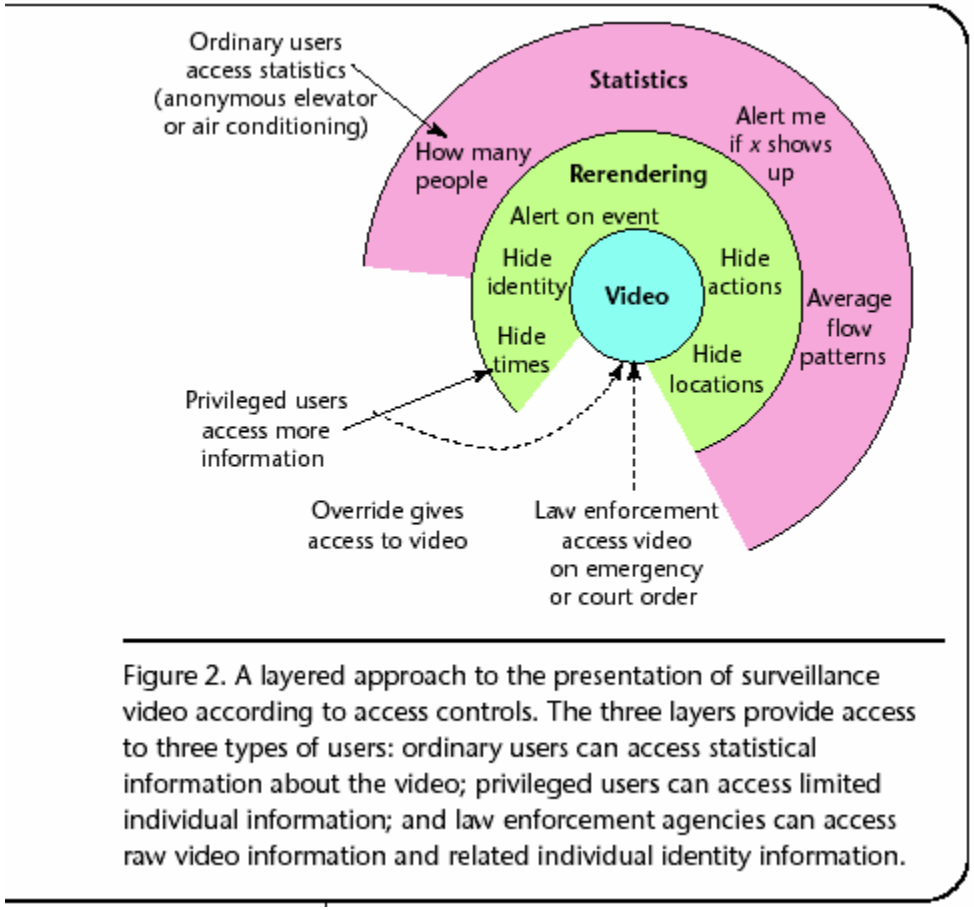


Figure 2. A layered approach to the presentation of surveillance video according to access controls. The three layers provide access to three types of users: ordinary users can access statistical information about the video; privileged users can access limited individual information; and law enforcement agencies can access raw video information and related individual identity information.

Architecture générale

- La prémisse principale est que le système peut automatiquement extraire les composants différents d'informations accordant un niveau d'autorisation d'accès.
- Le déchiffre a besoin d'une autorisation

1. Le système d'encodage se compose de trois types:
   - Analyse des vidéos: extraire les informations différentes (arrière-plan, objets mobiles, les caractéristiques des objets,…)
   - Transmission: transmettre les informations extraites
   - Sous-système: chiffrer les informations de façon différentes (chaque clé ouvert une scène différente)
2. Le système de décodage se compose de l'utilisateur interface et les sous systèmes synthétiques. Les utilisateur donne une requête, ensuite le système utilise cette requête avec le droit d'accès de cet utilisateur afin de déchiffrer les informations correspondantes.

Analyse des vidéos

- Afin de présenter les scènes différentes dépend à la situation et au type d'utilisateur
- En utilisant les algorithmes de vision par ordinateur pour « comprendre » les vidéos, extraire les informations utiles, distinguer l'arrière-plan et le premier plan, séparer les gens des véhicules,…
- Chaque objet extrait est stocké avec ses attributs tels qu'une type, une location, un temps,.. Il est aussi suivi par les images consécutives.
- Pour la transmission, il doit d'abord sélecter les informations souhaitées extraites de vidéo. On peut utiliser l'algorithme de bruit, brouillage or flou pour prévenir les informations privées.
- Pour protéger et restreindre les informations, on utilise l'approche de trois fronts en utilisant la transmission, le résumé et le chiffre pour délivrer les informations correspondantes à un utilisateur.
- Le système assure que un utilisateur ne peut pas accéder à plusieurs chaînes pour reconstruire une information complète d'objet.

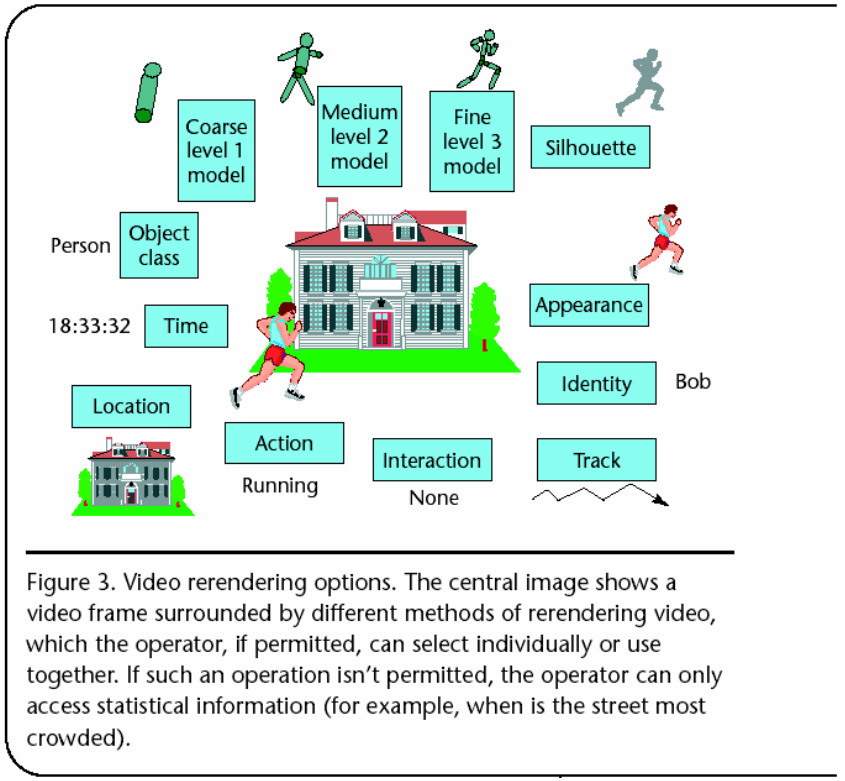


Figure 3. Video rerendering options. The central image shows a video frame surrounded by different methods of rerendering video, which the operator, if permitted, can select individually or use together. If such an operation isn't permitted, the operator can only access statistical information (for example, when is the street most crowded).

Caméra privé

- Ce sont les vidéosurveillances mais ils ont capacité de préserver les informations privées.
- Ils analysent, chiffrent les informations avant de les transmettre.
- On peut limiter les fonctions des caméras privés pour qu'ils puissiez seulement produire les images souhaitées limitées.

Garantie des informations privées

- Le système abordé n'est pas parfait, il reste encore deux erreurs:
  - Rater de détecter un objet or un événement
  - Faute d'alarme
- Un système sensitif trop haute a certaines fautes de détection mais trop d'alarme, tandis qu'un système sensitif bas a peu d'alarme mais il peut faire une faute de détecter un événement lors qu'il apparaît. Donc, on doit estimer tous les deux aspects.
- En tous cas, si on ne peut pas trouver les algorithmes efficaces pour préserver les informations privées, l'utilisation humain est plus difficile et plus coûteux.

Augmentation d'acceptation publiques

- Le modèle proposé est une option pour les vidéosurveillances, il observe les règlements exigés afin d'avoir l'acceptation publique
- Registrer le nombre d'identification des caméras sur Internet où les personnes peuvent confirmer la certification du système.
- Comme **les « CNIL » européennes précisent les règles applicables aux moteurs de recherche**.)

Conclusion

- La vidéosurveillance est une domaine potentiel pour améliorer la société moderne.
- Mais on doit encore faire les recherches pour trouver une façon plus efficace pour assurer toutes les deux aspects: publique et privée.
- Vision par ordinateur sera un domaine de pointe des scientifiques dans le futur proche.