N° d'ordre : 28 / RS / TCO Année Universitaire : 2013 / 2014

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME de LICENCE

Domaine : Sciences de l'ingénieur
Mention : Télécommunication
Parcours : Réseaux et Système (RS)

par : **RATOVO Fenosoa**

SECURISATION PAR TELESURVEILLANCE

Soutenu le **jeudi 05 Mars 2015** devant la Commission d'Examen composée de :

Président :
M. RAKOTONDRAINA Tahina Ezéchiel

Examinateurs :
M. RATSIMBAZAFY Andriamanga
M. RANDRIARIJAONA Lucien Elino
M. BOTO ANDRIANANDRASANA Jean Espérant

Directeur de mémoire :
M. RAKOTOMALALA Mamy Alain

REMERCIEMENTS

Je tiens à louer le Seigneur et Lui rendre Gloire pour toutes les bénédictions et interventions qu'Il a témoignées dans ma vie.

Je tiens également à remercier toutes les personnes qui ont contribué à la réalisation de ce présent mémoire. Cordialement à :

- Monsieur ANDRIANARY Philippe Antoine, Professeur Titulaire, Directeur de l'Ecole Supérieure Polytechnique d'Antananarivo ;
- Monsieur RAKOTOMALALA Mamy Alain, Maître de conférences, Chef de Département Télécommunication et Directeur de ce mémoire, pour le temps qu'il m'a accordé, pour son aide et ses conseils inestimables durant la préparation de ce travail

Ensuite mes vifs et sincères remerciements sont adressés aux enseignants qui sont membres du jury de cette soutenance malgré leurs obligations:

- Monsieur RAKOTONDRAINA Tahina Ezéchiel, Maître de conférences au sein de l'ESPA qui me fait l'honneur de présider le jury de soutenance de ce mémoire
- Monsieur RATSIMBAZAFY Andriamanga, Maître de conférences au sein de l'ESPA
- Monsieur RANDRIARIJAONA Lucien Elino, Assistant d'enseignement supérieur et de recherche
- Monsieur BOTO ANDRIANANDRASANA Jean Espérant, Assistant d'enseignement supérieur et de recherche au sein de l'ESPA

J'adresse mes sincères remerciements à tous les enseignants du département Télécommunication, les enseignants de l'Ecole Supérieure Polytechnique d'Antananarivo, les intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions.

Je ne saurais oublier d'exprimer un chaleureux remerciement envers toute ma famille pour leur soutien tant bien moral que matériel et qui m'a permis de poursuivre mes études.

Et enfin je remercie tous mes proches qui ont contribué, de près ou de loin à l'élaboration du présent mémoire.

TABLE DES MATIERES

ABREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
AGCH	Access Grant Channel
AUC	Authentification Center
BCH	Broadcast Channel
BCCH	Broadcast Control Channel
Bps	Bit per second
BSC	Base Station Controller
BTS	Base Transceiver Station
CCITT	Comité Consultatif International de Téléphonie et de Télégraphie
CCTV	Closed Circuit Television
CD-ROM	Compact Disc - Read Only Memory
CD	Compact Disc
CMJN	Cyan Magenta Jaune Noire
CMYK	Cyan Magenta Yellow Key
DAO	Dessin Assisté par Ordinateur
DSSS	Direct Sequence Spread Spectrum
DVR	Digital Video Recorder
FHSS	Frequency-Hopping Spread Spectrum
Ghz	Gigahertz
GND	Ground
GSM	Global System for Mobile Communication
HLR	Home Location Register
HSL	Hue Saturation Lightness
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
JRE	Java Runtime Environment

JVM	Java Virtual Machine
LLC	Logical Link Control
LUT	Look-Up Table
MAC	Media Access Control
Mbps	Megabits per second
MSC	Mobile Switching Center
NRZI	Non Return to Zero Inverted
NVR	Network Video Recorder
OCCTV	Open Closed Circuit Television
OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open Systems Interconnection
PA	Point d'accès
PIN	Personal Identification Number
PC	Personal Computer
PDA	Personal Digital Assistant
PPP	Point Par Pouce
RACH	Random Access Channel
RGB	Red Green Blue
RVB	Rouge Vert Bleu
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Center
TDMA	Time Division Multiple Access
TSL	Teinte Saturation Lumière
UIT	Union Internationale de la Télécommunication
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLR	Visitor Location Register
Wi-Fi	Wireless-Fidelity

WPAN	Wireless Personal Area Network
XML	Extensible Markup Language

INTRODUCTION GENERALE

De nos jours, la prédominance de l'insécurité, des vols et des attentats fait partie de la vie quotidienne des gens. Chaque individu vit dans l'inquiétude et la frustration en raison de l'incertitude sur les informations concernant la sécurisation de leur bien voire même leur vie. Cependant, à présent ces temps où les incertitudes dominaient sont révolus. Ce projet consiste justement à présenter une application servant à résoudre ces problèmes. En effet, cette application en question se base sur un système de sécurisation à distance dont la principale particularité est la possibilité de s'affranchir des problèmes liés à la distance. La manipulation de cette dernière peut être effectuée aussi bien par de simples utilisateurs que des adeptes de la nouvelle technologie.

Le domaine de la télécommunication n'a cessé de subir des évolutions de grandes envergures ayant avantagé la télésurveillance. La télécommunication fournit divers moyens mettant en profit l'utilisation d'un système de télésurveillance. Les équipements de télécommunication offrent et établissent un système de transmission fiable, sécurisé, rapide tout en respectant la confidentialité.

Ce mémoire qui s'intitule « Sécurisation par télésurveillance » se divise en quatre chapitres.

Le premier chapitre expliquera les informations théoriques concernant la télésurveillance ainsi que son utilisation au niveau d'une entreprise ou à usage personnel.

Le second chapitre parlera des différents procédés utiles pour la manipulation des images. Dans ce chapitre, les notions générales sur les images ainsi que la détection de mouvement seront évoquées.

Dans le troisième chapitre, on parlera des différents moyens, techniques et matériels mis en œuvre pour le bon fonctionnement de l'application élaborée. Parmi ces techniques se trouvent les différentes technologies de réseau sans fils et les ports de communication.

Le dernier chapitre expliquera en détails la réalisation proprement dite.

CHAPITRE 1

LA TELESURVEILLANCE

1.1 Introduction

La télésurveillance est une technique mise en œuvre afin de surveiller à distance des lieux, des machines ou bien des individus. Tout cela étant effectué dans le but de limiter voire même empêcher toute tentative de vol ou d'infraction. Depuis le XXIe siècle, son utilisation a été justifiée comme étant un moyen de lutte contre le terrorisme ainsi qu'un instrument de prévention contre la délinquance dans les villes. Un des types les plus connus de la télésurveillance connait actuellement un énorme succès : la vidéosurveillance. Désignée parfois par le sigle CCTV (Closed-Circuit Television), la vidéosurveillance est un système de caméras et de transmission d'images, disposé dans un espace public ou privé dans le but de le surveiller à distance.

1.2 Historique

Depuis 1939 à 1945, durant la Seconde Guerre Mondiale, les Allemands ont déjà utilisé le principe de la vidéosurveillance ainsi que le contrôle à distance. Mais elles n'ont été publiquement exploitées qu'à partir du moment où le système fut industrialisé, mettant ainsi le rôle des opérateurs en avant. Au début, les installations ne comportaient que des caméras et des écrans. Ensuite est apparu le matériel d'enregistrement permettant un archivage des scènes enregistrées. Puis l'avènement de l'ère numérique n'a fait que doper le secteur de la vidéosurveillance. [1]

1.2.1 Concept romanesque anticipatoire

Selon Antoine de Saint-Exupéry, écrivain et aviateur français, « fais de ta vie un rêve, et d'un rêve une réalité ». Cette citation montre à quel point l'influence de l'imagination peut avoir des conséquences sur la vie humaine. Dès 1949, l'idée innovatrice de la télésurveillance a commencé à faire irruption dans le cœur du monde. George Orwell, écrivain anglais, réussit à faire vivre l'idée en utilisant son roman d'anticipation intitulé « 1984 » comme moyen de communication. Ce dernier

plonge en effet les lecteurs dans un univers où le personnage principal est en mesure de surveiller toute une population grâce à un immense parc de caméras disséminées partout dans la ville. [1]

1.2.2 Approche technique

Un groupe international d'origine allemande spécialisé dans les hautes technologies, nommé Siemens, a mis en place le premier système de vidéosurveillance en 1942. L'objectif de cette installation ayant été de pouvoir observer des fusées. La mise en place d'un tel système requiert l'utilisation des matériels adéquats, surtout la caméra. La première caméra vidéo portative au monde date des années 1970 et depuis elle n'a cessé de connaître de nombreuses évolutions tant en quantité qu'en qualité. En effet, les caméras actuelles les plus performantes sont de type numérique, en couleur et offrent de nombreuses configurations.

1.3 Architecture d'une installation de vidéosurveillance

1.3.1 Vidéosurveillance en circuit fermé ou CCTV

Dans une installation CCTV ou Closed Circuit Television, le système est constitué d'un réseau de caméras et de moniteurs appartenant à une structure ou organisation n'ayant pas pour vocation de diffuser les images hors de ses murs. Il est alors valable pour les professionnels ne souhaitant pas diffuser en temps réel les images en dehors d'une entreprise. L'émission et la réception n'intéresse que celui qui est relié au réseau. Le pays disposant du plus grand nombre de caméras installées sur son territoire est la Grande Bretagne et ce phénomène commence à atteindre la France. Le CCTV est, historiquement, le premier système de vidéosurveillance mais l'évolution technologique de plus en plus complexe a permis une nette amélioration de ce système (caméras couleurs, enregistreur DVD, . . .). [2]

1.3.2 Vidéosurveillance en circuit ouvert ou OCCTV

Le rôle de la vidéosurveillance est d'accomplir une tâche bien définie de sécurisation. Pour l'installation en circuit ouvert ou OCCTV (Open Closed Circuit Television), le système est connecté à un réseau extérieur par l'intermédiaire d'internet. Grâce à ce système, l'utilisateur peut accéder à

son système à distance et en toute sécurité. En effet, ce procédé permet l'accès à de nombreuses fonctionnalités telles que : la surveillance de locaux à distance, la télésurveillance, surveillance multi-sites . . . Comme pour le cas du CCTV, des progrès ont aussi été effectués dans ce secteur par l'intermédiaire des technologies électroniques, informatiques et télécoms. [2]

1.4 Fonctions d'une installation

Dans une installation de vidéosurveillance, trois fonctions importantes et interdépendantes sont rencontrées : réception, gestion et visualisation.

Figure 1.01: Synoptique de l'installation de vidéosurveillance

1.4.1 Acquisition d'images

La caméra est l'élément fondamental du système de vidéosurveillance. Le choix sur le type de caméras se fera en fonction de l'environnement et des besoins de l'utilisateur. On distinguera entre autres :

- Des caméras couleur ou noir et blanc
- Des caméras à haute définition
- Des caméras couleur commutable noir et blanc
- Des caméras fixes, mobiles, discrètes
- Des caméras intérieures ou extérieures

Ces caméras associées à une machine hôte assurent l'acquisition des images à traiter.

1.4.2 Détection de mouvement

Cette fonction se sert des données obtenues par l'acquisition d'images pour travailler. Les détails concernant cette technique seront expliqués dans le prochain chapitre.

Différentes techniques de gestion permettent, en fonction des besoins d'exploitation, d'afficher une ou plusieurs images sur un ou plusieurs écrans. Ce type d'affichage se fera au travers de différents matériels prédéfinis lors de l'étude et correspondra aux besoins exprimés par le client. C'est dans cette partie que viendra se greffer le pupitre de télécommande des caméras mobiles. L'accomplissement de cette tâche peut aussi s'effectuer à l'aide de différents matériels tant software que hardware.

1.4.3 Présentation des informations

L'utilité de cette fonction est surtout remarquée au niveau du poste de garde ou du PC de sécurité. Mais au cas où il y a absence de ce dernier, la charge qu'il doit effectuer est attribuée à un autre service quelconque.

La première étape d'une étude d'installation de vidéosurveillance consiste à déterminer quelles seront les zones à surveiller ; à partir de cette étape, on déterminera la nature des caméras en prenant en compte l'environnement ; ensuite, on étudiera leur positionnement, cette phase nécessitant de réfléchir au cheminement des câbles en concertation avec l'utilisateur final. Dès que les voies de transmission aient été déterminées et que l'emplacement de la vidéo ait été fixé, il conviendrait de présenter les différentes solutions du système et de décrire les différents scénarios.

1.5 Principes physiques et techniques

La qualité des images reçues par une caméra dépend étroitement de la lumière et de l'éclairage présent dans le site concerné. Il est alors nécessaire de comprendre ces deux notions pour pouvoir mieux cernés le sujet.

1.5.1 La lumière

L'œil humain est capable de voir les ondes électromagnétiques dont la longueur d'onde est comprise entre 380 nm et 780 nm. [3] Et en fonction de cette longueur d'onde λ dépend la couleur de l'onde lumineuse dont voici quelques exemples :

- λ=470 nm correspond au bleu
- λ=575 nm correspond au jaune

- λ=500 nm correspond au cyan
- λ=680 nm correspond au rouge

La lumière du soleil, appelée aussi « lumière blanche » est une association de couleurs. En effet, la lumière blanche traversant une gouttelette subit une décomposition. Ce procédé conduit ainsi à l'apparition de l'arc-en-ciel. Cela est étroitement semblable à la décomposition de la lumière par l'intermédiaire d'un prisme.

Toutefois, il est également possible de synthétiser une couleur donnée en combinant différentes couleurs. Il existe deux types de synthèse :

- la synthèse additive :

Cette méthode consiste à ajouter différentes composantes de la lumière dès leur émission. Une technique très connue est l'utilisation des couleurs rouge, vert et bleu ou couleurs RVB permettant la reconstitution de tout le spectre des couleurs visibles dans une télévision.

- la synthèse soustractive :

Ce type de synthèse, quant à lui, consiste à éclairer une surface ayant la propriété d'absorber certaines couleurs et d'en réfléchir d'autres. Les couleurs reflétées, en se combinant, donnent une couleur visible.

Au-dessus de 780 nm se trouvent les infrarouges et en dessous de 380 nm se trouvent les rayonnements tels que les ultraviolets.

1.5.2 L'éclairage

1.5.2.1 Source de lumière directe

a. Lumière naturelle

La lumière naturelle subit des variations importantes en passant du jour à la nuit et suivant les périodes de l'année.

b. Lumière artificielle

La lumière artificielle est utilisée pour compenser la faible luminosité locale souvent due à l'insuffisance de l'éclairage de la lumière naturelle. Aujourd'hui, la plupart des projecteurs utilisés

appliquent la technologie de l'infrarouge. Les projecteurs à infrarouges sont en fait des projecteurs de lumière blanche équipés de filtre laissant passer la lumière infrarouge mais coupant la lumière blanche, visible par l'œil humain. Ainsi, on distingue deux principaux types d'éclairage :

- le premier type de source sera dans le domaine spectral du visible
- le deuxième dans le domaine de l'infrarouge invisible pour l'œil humain.

1.5.2.2 Source indirecte

Une des caractéristiques de la lumière est qu'elle se réfléchit différemment suivant la nature et la structure de l'élément réfléchissant. La gamme des éclairements précédents ne se rencontre jamais au complet dans une scène réelle. Les variations de luminance d'un objet donné sont dues d'une part aux variations d'éclairement, atténuées par les lumières réfléchies et, d'autre part par les variations de réflectivité, les noirs n'étant jamais à réflectivité nulle.

Bitume	5%
Terre végétale	7%
Gravier	13%
Arbres	20%
Briques	25%
Bétons	25%
Bâtiments	40%
Herbe verte	40%
Aluminium	65%
Neige	70%
Vitre	70%
Peinture blanche	75%

Tableau 1.01: Valeurs moyennes de réflexion de différents composants

1.5.2.3 Critères de sélection

Pour les applications de sécurité, l'éclairage horizontal est généralement de type infrarouge et l'éclairage vertical est de type visible.

Type d'éclairage Éclairage horizontal	Avantages	Inconvénients
Visible	Un seul projecteur	Éblouissement possible face au projecteur
	Coût de pose réduit	Éclairage non uniforme
	Coût matériel réduit	Éclairage non uniforme
Infrarouge	Un seul projecteur	Moins bon rendement
	Coût de pose réduit	Coût filtre infrarouge
	Discrétion	Éclairage non uniforme
Éclairage vertical		
Visible	Éclairage uniforme	Nombre de points d'éclairage
	Bon rendement	Pose plus coûteuse
	Dissuasion	Écrasement des images
Infrarouge	Éclairage uniforme	Coût très important
	Discrétion	Écrasement des images

Tableau 1.02: Critères de sélection

1.5.3 Les différents types de transmission

Le protocole IP est un moyen de communication permettant à différents équipements, formant un réseau, d'échanger des données. Trois types de transmission de la communication existent : transmission unicast, transmission multicast et transmission broadcast. [4]

1.5.3.1 Unicast

L'unicast est un type d'échange de données de poste à poste également appelé peer to peer. Ce type d'échange est représenté par la figure 1.02.

Figure 1.02: Communication unicast

1.5.3.2 Multicast

Le multicast est un type de transmission permettant à la même information d'être transmise simultanément à un nombre défini de récepteurs ou à un groupe d'utilisateurs bien défini. Par exemple, les images provenant d'une caméra quelconque d'une installation CCTV peuvent être visualisées en même temps par différents récepteurs. La figure 1.03 illustre ce type de transmission.

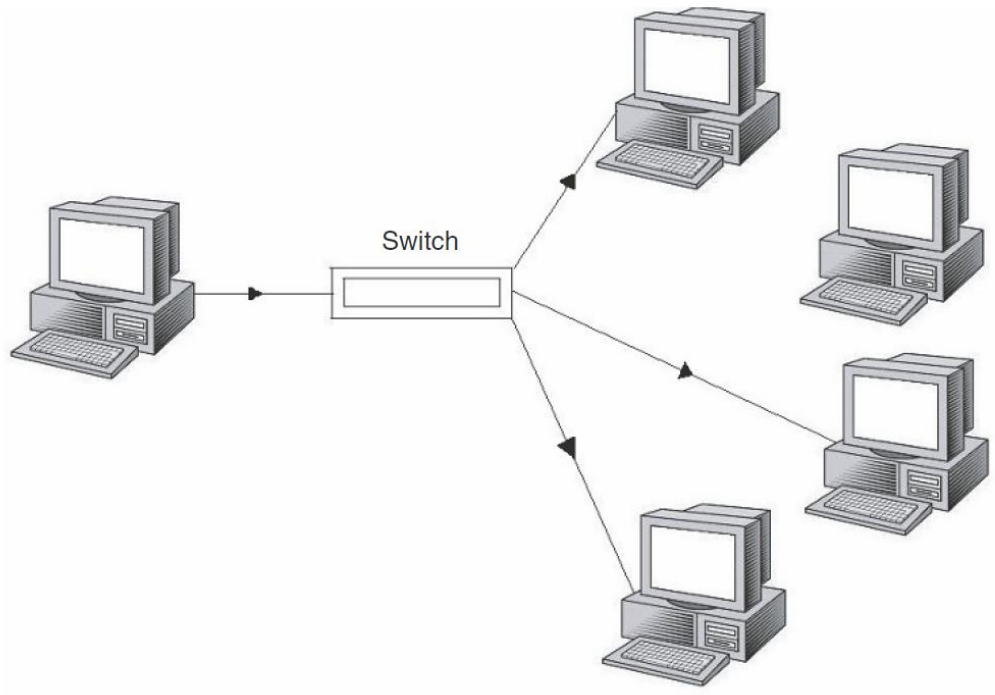

Figure 1.03: Communication multicast

1.5.3.3 Broadcast

Ce type de transmission consiste à envoyer les données à tous les récepteurs ou les utilisateurs sans exception comme le montre la figure 1.04.

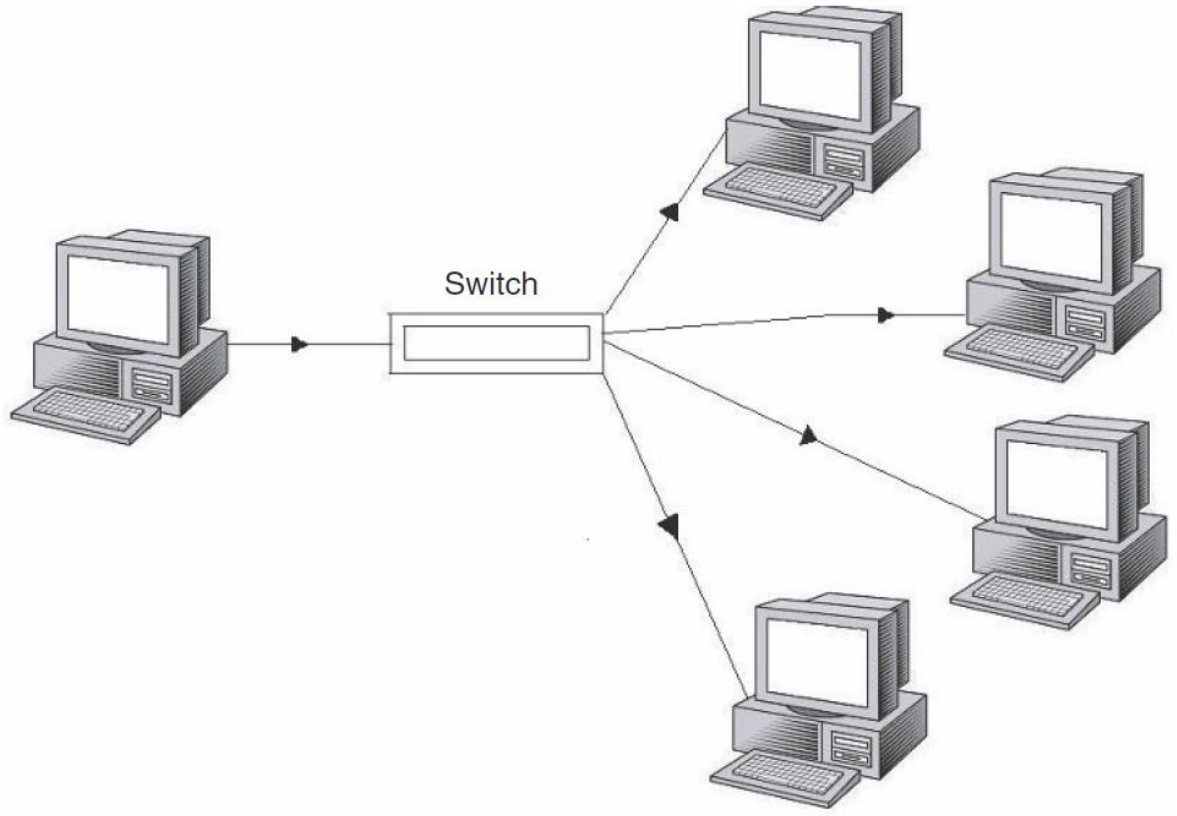

Figure 1.04: Communication broadcast

1.6 La télésurveillance proprement dite

Différents secteurs peuvent être sécurisés grâce à la vidéosurveillance à distance, dont voici quelques exemples :

- Etablissements privés (gares, hôpitaux, . . .)
- Bâtiments publics (mairie, centre administratif, . . .)

- Les évènements tels que les spectacles et les évènements sportifs
- Les sites professionnels (bureaux, entrepôts logistiques, . . .)
- Habitations privées (maison, appartement, . . .)
- Les produits à forte valeur

1.6.1 Sécurisation par simple gestion des alarmes

La démarche prise par cette sécurisation peut se dérouler suivant deux cas:

- En cas d'alarme, le télésurveilleur informe le client. La décision d'intervention est alors octroyée au client. Ce cas entraîne une prise de risque voire des dérangements intempestifs.
- Le télésurveilleur informe le service de gardiennage qui dépêche une patrouille sur le site entraînant des coûts.

Ces deux moyens d'intervention allongent le temps de réaction, ce qui peut entraîner de graves préjudices. Un moyen permet de résoudre cet inconvénient : l'utilisation de la levée de doute vidéo à distance.

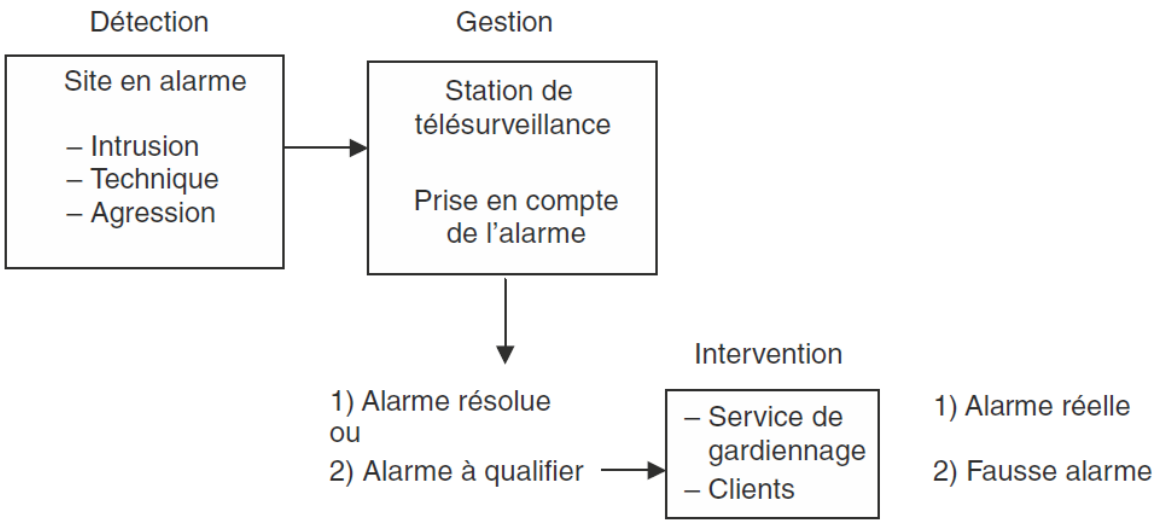

Figure 1.05: Synoptique d'une gestion d'alarme

1.6.2 Sécurisation par gestion des alarmes avec levée de doute vidéo

Le grand avantage de la levée de doute vidéo concerne la justification des demandes d'intervention des forces de l'ordre grâce à la confirmation visuelle des menaces.

La levée de doute vidéo permet, entre autres, d'éviter les interventions intempestives tout en améliorant :

- l'adaptation des moyens mis en œuvre en cas d'alarme confirmée et la coordination de l'intervention avec les forces de l'ordre
- l'application des consignes établies avec le client, le contact des forces de l'ordre ou d'une structure de gardiennage qui dépêche un agent de sécurité sur site.

La figure 1.06 illustre ce type de sécurisation.

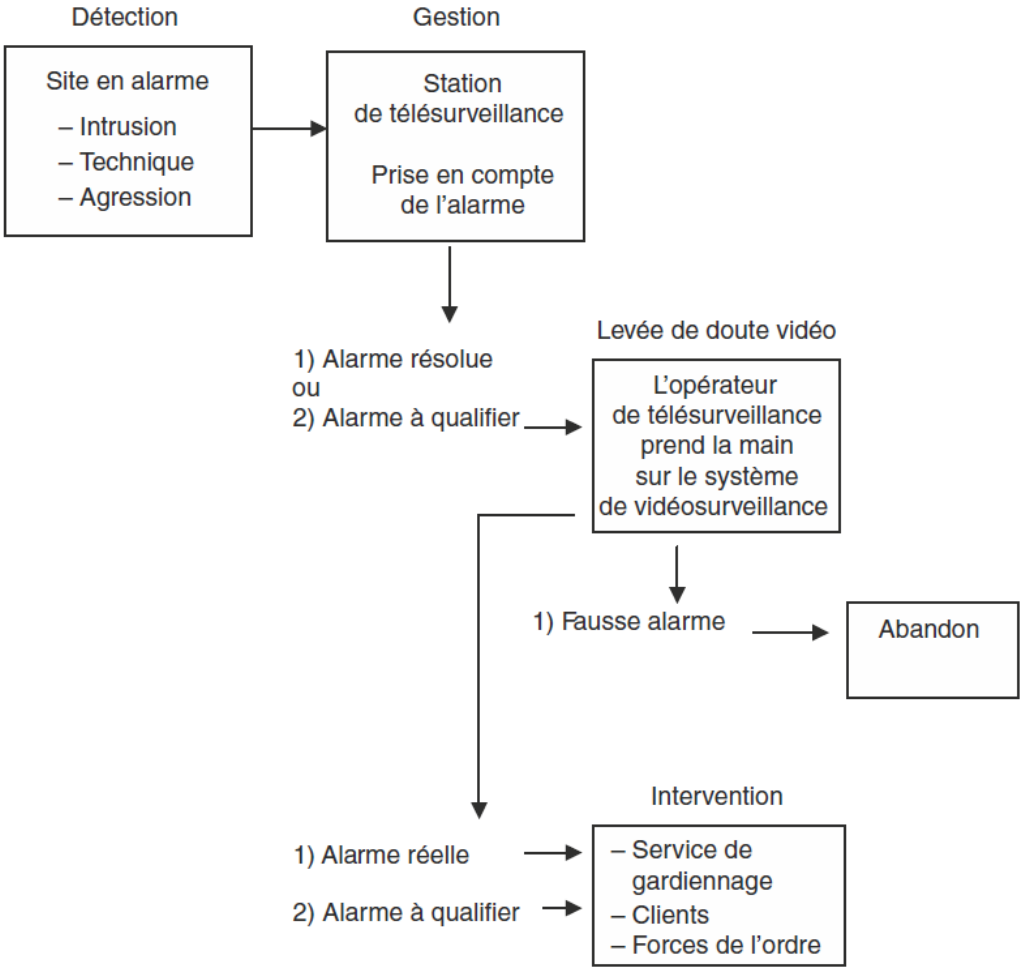

Figure 1.06: Gestion d'une alarme avec levée de doute vidéo

1.7 Domaines d’utilisation de la vidéosurveillance

1.7.1 Domaines publics

La vidéosurveillance dans les lieux publics améliore le niveau de sécurisation et contribue au bon déroulement de la vie quotidienne. En effet, elle apporte une aide irréfutable au maintien de l’ordre et de la paix dans un contexte urbain, que ce soit dans un parking, un espace public, lors de manifestations culturelles et d'événements ainsi que dans le cadre de la protection de bâtiments fortement fréquentés tels que les hôpitaux, écoles, universités ou églises.

1.7.2 Bâtiments industriels et commerciaux

La vidéosurveillance ou CCTV apporte aussi une grande aide aux bâtiments industriels et commerciaux. En plus des surveillances du périmètre et de l’enveloppe extérieure, les systèmes vidéo permettent aussi l’optimisation des processus et de la sécurité de travail. Effectivement, l’évolution des technologies a renforcé l’effet de dissuasion contre les malfaiteurs ; l’entrée en scène du système de reconnaissance faciale permet, en effet, une simple identification de l’individu en question. Elle apporte aussi d’autres avantages tels que : le suivi efficace de la logistique et du stockage, la surveillance du parking pour connaître l’identité des personnes ayant été présentes sur le site, la sécurisation des bureaux et des bâtiments commerciaux ainsi que la protection des secrets commerciaux.

1.7.3 Les foyers privés

La vidéosurveillance n’est pas seulement réservée aux banques, aux casinos ou aux grandes entreprises ; elle est, aujourd’hui, accessible à toute personne qui s’y intéresse. Et selon les besoins de chacun, des solutions leur sont proposées.

1.7.3.1 Sécurisation de l’extérieur

Grâce au CCTV, l’utilisateur est toujours informé de ce qui se passe sur son terrain, et le simple fait de connaître le niveau de sécurisation d’une maison peut servir d’outil de dissuasion pour les malfaiteurs. En effet, ils se tiendront à distance par peur d’être reconnus ou arrêtés.

1.7.3.2 Sécurisation de la zone d'entrée et de l'intérieur

Même si les cambrioleurs préfèrent les fenêtres, les portes et les serrures de portes sont souvent la cible d'attaques, par exemple par le perçage des serrures. Ainsi, l'installation du système au niveau de l'entrée avise le propriétaire de la présence d'un individu à sa porte, lui permettant ainsi d'effectuer les actions appropriées. D'un autre côté, l'utilisation du système vidéo interne surveille aussi l'action de tout individu du site, et ceci, même si le propriétaire se trouve à plusieurs lieux de son foyer.

1.8 Vidéosurveillance en entreprise

Cette application est aussi bien utile pour les particuliers que pour les entreprises. En effet, le niveau de sécurisation ainsi que les matériels qui lui sont associés témoignent son efficacité.

1.8.1 Fonctionnement sur IP

Outre l'utilisation de caméras ordinaires, cette application prend aussi en compte les caméras IP. La technologie IP permet une simple utilisation qui peut même être appliquée via une liaison Wi-Fi. Mais l'un des gros problèmes rencontrés lors de ce genre de cas est le problème de congestion. La congestion d'un réseau informatique est la condition dans laquelle une augmentation du trafic provoque un ralentissement global de celui-ci. Souvent, elle est causée suite à un mauvais paramétrage au niveau de la compression et du nombre d'images par seconde des caméras. Or, ce problème a été nettement corrigé grâce à l'utilisation d'une technique de filtrage des images enregistrées.

Les principaux avantages du système IP sont :

- La facilité de stockage :
  Les images sont numérisées et enregistrées sur un serveur, alors elles peuvent être facilement manipulées et sont plus sécurisées.

- La mobilité dans l'utilisation :
  Grâce à l'interconnexion des différents appareils ainsi qu'à l'utilisation d'un routeur, la télésurveillance peut être effectuée depuis n'importe quel ordinateur du réseau.

- La réduction des coûts :

  Les algorithmes employés permettent la réduction de l'espace de stockage, ainsi que la puissance informatique nécessaire, d'où la réduction des frais d'infrastructure et de maintenance.

1.8.2 Respect du cadre légal

En premier lieu, un système de vidéosurveillance ne peut être installé avec le seul objectif de contrôler en permanence l'activité de ses employés. L'employeur doit, en premier lieu, témoigner d'un intérêt légitime à la mise en place d'un système de surveillance. Il peut s'agir de la nécessité de protéger des personnes ou des biens, ou de se prémunir contre des risques divers, tels que le vol.

Ensuite, le système doit obligatoirement être proportionné aux regards des intérêts protégés. Ceci dans le but de protéger le droit de chacun au respect de sa vie privée.

En supplément, d'autres lois doivent être connues afin d'établir un système de vidéosurveillance au sein d'une entreprise. [5]

1.8.2.1 Loi Pasqua

Les formalités à remplir et les lois régissant le système de vidéosurveillance dépend du lieu placé sous surveillance. Il est alors nécessaire de comprendre la distinction entre un lieu public et un lieu privé :

- Lieu public ou ouvert au public : tout lieu du secteur public ou du secteur privé où le public peut accéder.
- Le lieu privé (lieu non ouvert au public) : tout lieu du secteur public ou du secteur privé où le public ne peut pas accéder.

Les entreprises ouvertes au public telles que les commerces, hôtels, sont concernées par la loi Pasqua, et doivent déclarer leur installation de vidéosurveillance à leur préfecture. Elles doivent remplir un formulaire ainsi qu'un dossier détaillant l'installation et ses caractéristiques (type de caméras, durée d'enregistrement, . . .), les zones filmées et l'accès aux données.

L'entreprise non ouverte au public, étant juridiquement un lieu privé, n'est pas concernée par la Loi Pasqua du 21 janvier 1995 relative à la vidéosurveillance. Cependant, si le champ des caméras porte sur une partie de la voie publique, une demande d'autorisation en préfecture est obligatoire.

1.8.2.2 Code du travail

Selon le code du travail, un employeur a le droit de surveiller ses salariés en ayant recours à un système de vidéosurveillance. Il est à noter que le code du travail prévoit une information individuelle et collective des salariés sur l'existence d'un traitement contenant des données personnelles les concernant. L'information doit être diffusée en amont de l'installation du dispositif et non après son démarrage.

1.9 Conclusion

Les rapides et prégnantes évolutions technologiques n'ont cessé d'influencer les comportements individuels et ceux des entreprises. Ces derniers veulent protéger au mieux leurs biens et toutes choses qui leurs sont précieuses. Et c'est là que la télésurveillance fait son apparition, elle subvient à leurs besoins. Selon les critères de chaque utilisateur, elle offre la solution adéquate. Et depuis une cinquantaine d'années, elle fait l'un des grands sujets imbriqués dans l'esprit des gens. Ceci étant surtout causé du fait que le niveau de sécurisation apporté par le système de vidéosurveillance atteint actuellement un échelon non négligeable.

CHAPITRE 2

SYSTEME D'ACQUISITION D'IMAGES

2.1 Introduction

Les images constituent des preuves visuelles importantes pour la mise en place d'un système de sécurisation. En effet, la suivie visuelle de tous les évènements se produisant dans un site donné améliore nettement l'efficacité de la sécurisation et permet ainsi, aux différents utilisateurs du système, de prendre les mesures adaptées à chaque cas. Mais pour mieux comprendre l'utilité des images, une étude approfondie sur ces dernières et des différents moyens pour les manipuler deviennent une nécessité.

2.2 Les images

2.2.1 Image numérique

L'appellation « **image numérique** » désigne toute image acquise, créée, traitée et stockée sous forme binaire :

- acquise par des convertisseurs analogique-numérique situés dans des dispositifs comme les scanners, les appareils photo ou les caméscopes numériques, les cartes d'acquisition vidéo qui numérisent directement une source comme la télévision
- créée directement par des programmes informatiques, grâce à une souris, des tablettes graphiques ou par de la modélisation 3D
- traitée grâce à des outils Graphique, de façon à la transformer, à en modifier la taille, les couleurs, d'y ajouter ou d'en supprimer des éléments, d'y appliquer des filtres variés, et tout autre traitement stockée sur un support informatique comme une clé USB, disque dur, CD-ROM [6]

2.2.2 Types d'images

2.2.2.1 Images matricielles ou Images Bitmap

Elle est composée d'une matrice (tableau) de points à plusieurs dimensions, chaque dimension représentant une dimension spatiale (hauteur, largeur, profondeur), temporelle (durée) ou autre (par exemple, un niveau de résolution).

2.2.2.2 Images 2D

Dans le cas des images à deux dimensions, les points sont appelés pixels. D'un point de vue mathématique, on considère l'image comme une fonction de $\mathbb{R}\ x\ \mathbb{R}$ dans $\mathbb{R}$ où le couplet d'entrée est considéré comme une position spatiale, le singleton de sortie comme un codage.

Ce type d'image s'adapte bien à l'affichage sur écran informatique, lui aussi orienté pixel. Il est en revanche peu adapté pour l'impression, car la résolution des écrans informatiques, généralement de 72 à 96 ppp (points par pouce) est bien inférieure à celle atteinte par les imprimantes, au moins 600 ppp aujourd'hui. L'image imprimée, si elle n'a pas une haute résolution, sera donc plus ou moins floue ou laissera apparaître des pixels carrés visibles.

2.2.2.3 Images 2D + t (vidéo), images 3D, images multi-résolution

Lorsqu'une image possède une composante temporelle, on parle d'animation. Dans le cas des images à trois dimensions, les points sont appelés des « voxels ». Ils représentent un volume. Ces cas sont une généralisation du cas 2D, la dimension supplémentaire représentant respectivement le temps, une dimension spatiale ou une échelle de résolution. D'un point de vue mathématique, il s'agit d'une fonction de $\mathbb{R}\ x\ \mathbb{R}\ x\ \mathbb{R}$ dans $\mathbb{R}$.

2.2.2.4 Images stéréoscopiques

Il s'agit d'un cas particulier dans lequel on travaille par couples d'images, ces derniers pouvant être de n'importe lequel des types précédents.

Il existe un grand nombre de sortes d'images stéréoscopiques, et un encore plus grand nombre de moyens pour les observer en relief, mais le codage recommandé par les organisations internationales de stéréoscopie est désigné comme « jps », c'est-à-dire un format jpg dans lequel les deux vues gauche et droite sont juxtaposées dans un même fichier, le plus souvent 2 048 × 768, chacune des deux vues étant inscrite dans un rectangle 1 024 × 768 et, si son rapport largeur sur hauteur n'est pas $\frac{4}{3}$, chaque vue est complétée dans ce rectangle par deux bandes noires symétriques, soit en haut et en bas, soit à gauche et à droite.

2.2.2.5 Images vectorielles

Le principe est de représenter les données de l'image par des formules géométriques qui vont pouvoir être décrites d'un point de vue mathématique. Cela signifie qu'au lieu de mémoriser une mosaïque de points élémentaires, on stocke la succession d'opérations conduisant au tracé. Par exemple, un dessin peut être mémorisé par l'ordinateur comme « une droite tracée entre les points (x_1, y_1) et (x_2, y_2) », puis « un cercle tracé de centre (x_3, y_3) et de rayon 30, de couleur rouge ».

L'avantage de ce type d'image est la possibilité de l'agrandir indéfiniment sans perdre la qualité initiale, ainsi qu'un faible encombrement. L'usage de prédilection de ce type d'images concerne les schémas qu'il est possible de générer avec certains logiciels de DAO (Dessin Assisté par Ordinateur) comme AutoCAD ou CATIA. Ce type d'images est aussi utilisé pour les animations Flash, utilisées sur Internet pour la création de bannières publicitaires, l'introduction de sites web, voire des sites web complets.

Étant donné que les moyens de visualisation d'images actuels comme les écrans d'ordinateur reposent essentiellement sur des images matricielles, les descriptions vectorielles (Fichiers) doivent préalablement être converties en descriptions matricielles avant d'être affichées comme images.

2.2.3 Définition et résolution

Les images matricielles sont également définies par leur définition et leur résolution.

La **définition** d'une image est définie par le nombre de points la composant. En image numérique, cela correspond au nombre de pixels qui composent l'image en hauteur (axe vertical) et en largeur (axe horizontal) : *200 pixels par 450 pixels* par exemple, abrégé en « 200 × 450 ».

La **résolution** d'une image est définie par un nombre de pixels par unité de longueur de la structure à numériser (classiquement en ppp). Ce paramètre est défini lors de la numérisation (passage de l'image sous forme binaire), et dépend principalement des caractéristiques du matériel utilisé lors de la numérisation. Plus le nombre de pixels par unité de longueur de la structure à numériser est élevé, plus la quantité d'information qui décrit cette structure est importante et plus la résolution est élevée. La résolution d'une image numérique définit le degré de détail de l'image. Ainsi, plus la résolution est élevée, meilleure est la restitution.

Cependant, pour une même dimension d'image, plus la résolution est élevée, plus le nombre de pixels composant l'image est grand. Le nombre de pixels est proportionnel au carré de la résolution, étant donné le caractère bidimensionnel de l'image : si la résolution est multipliée par deux, le nombre de pixels est multiplié par quatre. Augmenter la résolution peut entraîner des temps de visualisation et d'impression plus longs, et conduire à une taille trop importante du fichier contenant l'image et à de la place excessive occupée en mémoire.

Figure 2.01: Exemple d'images avec différentes résolutions

2.2.4 Représentation des couleurs

Il existe plusieurs modes de codage informatique des couleurs. Le plus utilisé pour le maniement des images est l'espace colorimétrique rouge, vert, bleu (RVB ou RGB - *red green blue*). Cet espace est basé sur une synthèse additive des couleurs, c'est-à-dire que le mélange des trois composantes

R, V, et B à leur valeur maximum donne du blanc, à l'instar de la lumière. Le mélange de ces trois couleurs à des proportions diverses permet de reproduire à l'écran une part importante du spectre visible, sans avoir à spécifier une multitude de fréquences lumineuses.

Il est à remarquer qu'il existe d'autres modes de représentation des couleurs :

- cyan, magenta, jaune, noir (CMJN ou CMYK) utilisé principalement pour l'impression, et basé sur une synthèse soustractive des couleurs ;
- teinte, saturation, luminance (TSL ou HSL), où la couleur est codée suivant le cercle des couleurs ;
- base de couleur optimale YUV, Y représentant la luminance, U et V deux chrominances orthogonales.

Les images bitmap en couleurs peuvent être représentées soit par une image dans laquelle la valeur du pixel est une combinaison linéaire des valeurs des trois composantes couleurs, soit par trois images représentant chacune une composante couleur. Dans le premier cas, selon le nombre de bits alloués pour le stockage d'une couleur de pixel, on distingue généralement les différents types d'images suivants :

2.2.4.1 Images 24 bits ou « couleurs vraies »

Il s'agit d'une appellation trompeuse car le monde numérique (fini, limité) ne peut pas rendre compte intégralement de la réalité (infinie). Le codage de la couleur est réalisé sur trois octets, chaque octet représentant la valeur d'une composante couleur par un entier de 0 à 255. Ces trois valeurs codent généralement la couleur dans l'espace RVB. Le nombre de couleurs différentes pouvant être ainsi représenté est de 256 × 256 × 256 possibilités, soit environ 16,7 millions de couleurs. Comme la différence de nuance entre deux couleurs très proches mais différentes dans ce mode de représentation est quasiment imperceptible pour l'œil humain, on considère commodément que ce système permet une restitution exacte des couleurs, c'est pourquoi on parle de « couleurs vraies ». Un exemple de composition de couleurs est représenté par la figure 2.02.

R	V	B	Couleur
0	0	0	noir
0	0	1	nuance de noir
255	0	0	rouge
0	255	0	vert
0	0	255	bleu
128	128	128	gris
255	255	255	blanc

Figure 2.02: Exemple de composition de couleurs RVB

Les images bitmap basées sur cette représentation peuvent rapidement occuper un espace de stockage considérable, chaque pixel nécessitant trois octets pour coder sa couleur.

2.2.4.2 Images à palettes, images en 256 couleurs (8 bits)

Pour réduire la place occupée par l'information de couleur, on utilise une *palette de couleurs* « attachée » à l'image. On parle alors de couleurs indexées : la valeur associée à un pixel ne véhicule plus la couleur effective du pixel, mais renvoie à l'entrée correspondant à cette valeur dans une table (ou palette) de couleurs appelée *look-up table* ou LUT en anglais, dans laquelle on dispose de la représentation complète de la couleur considérée.

Selon le nombre de couleurs présentes dans l'image, on peut ainsi gagner une place non négligeable : on considère en pratique que 256 couleurs parmi les 16 millions de couleurs 24 bits sont suffisantes. Pour les coder, on aura donc une palette occupant 24 bits × 256 entrées, soit 3 × 256 octets, et les pixels de l'image seront associés à des index codés sur un octet. L'occupation d'une telle image est donc de 1 octet par pixel plus la LUT, ce qui représente un peu plus du tiers de la place occupée par une image en couleurs 24 bits (plus l'image contient de pixels, plus le gain de place est important, la limite étant le tiers de la place occupée par l'image en couleurs vraies).

Une autre méthode existante consiste à se passer de palette et de coder directement les trois couleurs en utilisant un octet : chaque composante couleur est codée sur deux bits, le bit restant peut servir

soit à gérer plus de couleurs sur une des composantes, soit à gérer la transparence du pixel. Avec cette méthode, on obtient des images bitmap avec un codage couleur effectivement limité à 8 bits, bien que la plage des couleurs possibles soit très réduite par rapport à celle qu'offre la méthode utilisant une palette.

Dans le cas des images en couleurs indexées, il est possible de spécifier que les pixels utilisant une des couleurs de la palette ne soient pas affichés lors de la lecture des données de l'image. Cette propriété de transparence est très utilisée pour les images des pages web, afin que la couleur de fond de l'image n'empêche pas la visualisation de l'arrière-plan de la page.

2.2.4.3 Images en teintes ou niveaux de gris

On ne code plus ici que le niveau de l'intensité lumineuse, généralement sur un octet (256 valeurs). Par convention, la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255 le blanc (intensité lumineuse maximale) :

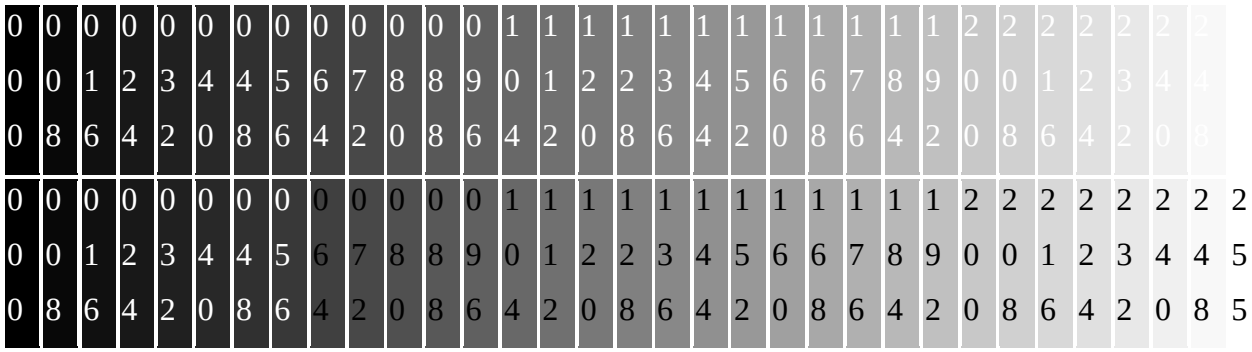

Figure 2.03: Couleurs obtenues pour les variations du niveau de gris

Ce procédé est fréquemment utilisé pour reproduire des photos en noir et blanc ou du texte dans certaines conditions, avec utilisation d'un filtre pour adoucir les contours afin d'obtenir des caractères plus lisses.

Ce codage de la simple intensité lumineuse est également utilisé pour le codage d'images couleurs : l'image est représentée par trois images d'intensité lumineuses, chacune se situant dans une composante distincte de l'espace colorimétrique.

2.3 Principe de la détection de mouvement

La détection de mouvement ou « motion detection » est un processus de détection d'un changement de position d'un objet par rapport à son environnement ou un changement de l'environnement par rapport à un objet.

La qualité d'une image dépend étroitement des caractéristiques du matériel utilisé. Lors de la détection de mouvement, la webcam capturera des images à intervalles réguliers. Et l'ordinateur effectuera les opérations nécessaires pour déterminer si 2 images sont identiques ou non. Il est à noter que, même pour une image immobile, la webcam percevra une légère variation. Ceci constitue un des facteurs qui fait de la « motion detection » une application assez complexe. Le traitement se fera en deux grandes parties : le découpage de l'image en plusieurs zones et la comparaison de chaque pixel.

- La comparaison se fait avec définition d'une marge d'erreur, cela implique qu'on ne peut se contenter de travailler en booléenne. En effet, l'utilisation d'une booléenne montrera, la plupart du temps, que les deux images sont différentes à cause de la variation perçue par la webcam, d'où la nécessité d'une marge d'erreur (ex : 10%). Une autre méthode permettant d'affiner le traitement consiste à retenir les images des x dernières secondes (ex : 5s) et de comparer l'image actuelle avec celles-là plutôt que celle qui la précède. Ce procédé permet entre autres de détecter un objet se déplaçant très lentement.
- Le découpage en zones donne une meilleure précision à la détection. Plus la taille de la partie étudiée est petite, plus les détails ainsi que les précisions accroissent.

  Dans une zone, on effectue l'opération de comparaison. Pour comparer 2 images, on compare les différentes proportions de rouge, vert et bleue (couleur RVB) entre les images. Ensuite, on calcule le delta E entre les 2 images et cela donne la possibilité de définir un seuil limite ou marge d'erreur, qui au-delà de celui-ci, l'application détectera un mouvement.

  Le delta E, est défini comme une mesure de différence entre deux couleurs.

$$\text{Delta E} = \sqrt{(\text{L1} - \text{L2})^2 + (\text{a1} - \text{a2})^2 + (\text{b1} - \text{b2})^2} \qquad (2.01)$$

Où

$L1, a1, b1$ sont les coordonnées dans l'espace colorimétrique de la première couleur à comparer et $L2, a2, b2$ celles de la seconde.

Il faut savoir que des couleurs ayant un même delta E sont perçues par l'œil humain comme ayant la même différence de couleur et que les delta E inférieurs à environ 5 correspondent à des couleurs perçues comme identiques à des yeux non exercés.

Il est à noter qu'il existe d'autres méthodes permettant d'effectuer une détection de mouvement comme l'utilisation de la méthode gaussienne s'appuyant sur le fait d'utiliser une différence gaussienne sur deux images, puis de comparer le résultat de cette différence.

2.4 Webcam

2.4.1 Généralités

Une webcam est une caméra conçue pour être utilisée comme un périphérique d'ordinateur, et qui produit une vidéo dont la finalité n'est pas d'atteindre une haute qualité, mais de pouvoir être transmise en direct au travers d'un réseau. Mais l'avancée technologique tend à normaliser la norme High Definition, mettant ainsi en valeur la gamme des hautes résolutions.

Pour se connecter à un ordinateur, une webcam peut utiliser divers moyens :

- le port USB
- les ports parallèle ou série, abandonné du fait du trop bas débit
- un réseau Ethernet ou Wi-Fi
- la liaison Bluetooth

Certains appareils tels que les téléphones portables ainsi que les appareils photos numériques intègrent également une fonction webcam. Et ceux qui n'en disposent pas peuvent être utilisés comme webcam s'ils disposent d'une sortie vidéo, et que l'ordinateur dispose d'une entrée vidéo.

Les images captées par une webcam sont principalement destinées à être transmises par le biais d'un réseau. Pour ne pas dépasser le débit d'un tel réseau, l'image produite est compressée pour obtenir une image de faible qualité, tant en définition qu'en taux de rafraîchissement, c'est-à-dire le nombre d'images par seconde. Ainsi, pour assurer une qualité d'image convenable, il est préférable de disposer d'une connexion à haut débit, par exemple ADSL.

2.4.2 Utilisations

La webcam peut filmer et produire un flux vidéo classique pouvant servir à la visiophonie, ou bien capturer périodiquement une image. Son usage pratique relève souvent de la communication, en particulier de la visioconférence, ainsi que de la vidéosurveillance, surtout de la détection de mouvement assurée par un programme analysant les différences entre les images successives. L'utilisation de la webcam pour la visiophonie se diffuse très largement pour les communications personnelles entre internautes via la messagerie instantanée, ou encore via des sites spécifiques.

2.5 Cameras IP

2.5.1 Vue globale

Une caméra IP ou caméra réseau est une caméra de surveillance utilisant le Protocole Internet pour transmettre des images et des signaux de commande via une liaison Fast Ethernet. Certaines caméras IP sont reliées à un enregistreur vidéo numérique (DVR) ou un enregistreur vidéo en réseau (NVR) pour former un système de surveillance vidéo. [7]

L'avantage des caméras IP est qu'elles permettent aux propriétaires et aux entreprises de consulter leurs caméras depuis n'importe quelle connexion internet via un ordinateur portable ou un téléphone 3G.

Une caméra IP peut être câblée avec du RJ45 vers un routeur ou « box ADSL », ce qui lui permet à la fois d'être alimentée et les images peuvent être visionnées sur le réseau, ou alors par Wi-Fi.

2.5.2 Avantages

Un système de vidéosurveillance numérique sur IP offre de nombreux avantages et des fonctionnalités avancées que ne peut pas offrir un système de vidéosurveillance analogique. Parmi ces avantages, citons l’accessibilité à distance, la haute qualité d’image, une meilleure évolutivité, ainsi qu’une flexibilité accrue.

2.5.2.1 Accessibilité à distance

Les caméras réseau et les encodeurs vidéo sont configurables et accessibles à distance, ce qui permet à plusieurs utilisateurs autorisés de visualiser à tout moment la vidéo en direct ou enregistrée depuis n'importe quel point du réseau à travers le monde. C'est un véritable atout lorsque les utilisateurs souhaitent qu'une société tierce, telle qu'une entreprise de sécurité, puisse également accéder à la vidéo. Avec un système CCTV analogique traditionnel, les utilisateurs doivent se trouver à un emplacement de contrôle spécifique sur site pour visualiser et gérer la vidéo, et l'accès vidéo hors site serait impossible sans un encodeur vidéo ou un enregistreur vidéo numérique réseau.

2.5.2.2 Images de haute qualité

Dans une application de vidéosurveillance, la qualité de l'image est essentielle pour capturer de manière claire tout incident en cours, et identifier les personnes ou objets impliqués. Avec la résolution mégapixel et le balayage progressif, une caméra réseau peut fournir une image de qualité et de résolution supérieures à celles d'une caméra analogique.

La qualité de l'image est également mieux conservée avec un système de vidéo sur IP qu'avec un système de surveillance analogique. Avec les systèmes analogiques qui utilisent un enregistreur numérique comme support d'enregistrement, de nombreuses conversions analogiques/ numériques ont lieu : tout d'abord, les signaux analogiques sont convertis en signaux numériques dans la caméra, puis de nouveau en signaux analogiques pour le transport ; ensuite, ces signaux analogiques sont numérisés en vue de leur enregistrement. La qualité des images capturées se dégrade à chaque conversion entre les formats analogique et numérique, et avec la distance de câblage. Plus la distance de transport des signaux vidéo analogiques est longue, plus ces signaux s'affaiblissent.

Avec un système d'IP-Surveillance entièrement numérique, les images d'une caméra réseau sont numérisées une seule fois et demeurent numériques, ce qui évite toute conversion inutile et toute dégradation de l'image due à la distance de transport sur le réseau. En outre, il est plus simple de stocker et d'extraire les images numériques, que dans le cas d'utilisation de bandes vidéo analogiques.

2.5.2.3 Evolutivité et flexibilité

Un système de vidéo sur IP peut évoluer avec les besoins de l'utilisateur. Les systèmes basés sur le protocole IP permettent à de nombreux encodeurs vidéo et caméras réseau de partager le même réseau câblé ou sans fil pour transmettre les données. Cela nous donne la possibilité d'ajouter au système autant de produits de vidéo sur IP qu'on le souhaite sans avoir à modifier l'infrastructure réseau de façon coûteuse ou significative.

2.6 Conclusion

Pour conclure, de nos jours la notion d'images ne peut être séparée du système de télésurveillance. Ce couple augmente le taux d'efficacité d'une application de sécurisation. Et associée à d'autres techniques telles que le réseau de la téléphonie mobile, la télésurveillance présente des avantages non négligeables. Ces différents faits montrent que l'utilisation des images dans une application de sécurisation permet à la fois l'affranchissement des limites engendrées par la distance et la suivie visuelle de tout évènement se déroulant dans un site.

CHAPITRE 3

SYSTEME DE TRANSMISSION

3.1 Introduction

Différents moyens permettent de résoudre les problèmes liés à la distance. Et ce chapitre consiste justement à expliquer en détails ces méthodes car elles jouent un rôle fondamental dans l'établissement d'un système de télésurveillance pratique et performant. En effet, la télésurveillance est le fait de pouvoir surveiller un site à distance. Alors les diverses techniques qui contribuent à l'élaboration d'un tel système seront ici détaillées.

3.2 Modem

Le modem est un périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'un réseau analogique comme une ligne téléphonique. Techniquement, l'appareil sert à convertir les données numériques de l'ordinateur en signal modulé, dit « analogique », transmissible par un réseau analogique et réciproquement.

3.2.1 Technologie du modem

Le modem est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via un support de transmission filaire. Les ordinateurs fonctionnent de façon numérique, ils utilisent le codage binaire. Les signaux numériques passent d'une valeur à une autre, il n'y a pas de milieu, de moitié, c'est du « Tout Ou Rien ». Par contre, les lignes téléphoniques sont analogiques. Les signaux analogiques n'évoluent pas « par pas », mais évoluent plutôt de façon continue. Le modem convertit alors en analogique l'information binaire provenant de l'ordinateur, afin de le moduler par la ligne téléphonique. Il effectue la modulation, cette dernière étant un codage des données numériques et synthèse d'un signal analogique qui est en général une fréquence porteuse modulée. L'opération de démodulation effectue l'opération inverse et permet au récepteur d'obtenir l'information numérique. Le mot « modem » est ainsi un acronyme pour « MOdulateur/DEModulateur ». [8] Le principe de fonctionnement du modem est illustré par la figure 3.01.

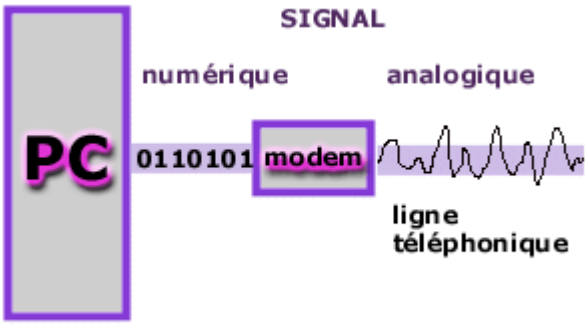

Figure 3.01: Fonctionnement d'un modem

3.2.2 Les standards de communication

La multiplication des modems a nécessité une standardisation des protocoles de communication par modem afin qu'ils parlent tous un langage commun. On appelle protocole le langage utilisé par les ordinateurs pour communiquer entre eux. C'est la raison pour laquelle deux organismes ont mis au point des standards de communication :

- Les laboratoires BELL, précurseurs en matière de télécommunication ;
- Le Comité consultatif international de téléphonie et de télégraphie (CCITT), renommé depuis 1990 en union internationale de la télécommunication (UIT).

L'UIT a pour but de définir les standards de communications internationaux. Les standards des modems peuvent se diviser en trois catégories :

- Les standards de modulation (par exemple *CCITT V.21*)
- Les standards de correction d'erreurs (par exemple *CCITT V.42*)
- Les standards de compression des données (par exemple *CCITT V.42bis*)

Le tableau 3.01 suivant montre des exemples de principaux standards de modem :

Standard de modulation	**Débit théorique**	**Mode**	**Description**
Bell 103	300 bps	Full duplex	Standard américain et canadien utilisant un codage à

			changement de fréquence. Il permet ainsi d'envoyer un bit par baud.
CCITT V.21	300 bps	Full duplex	Standard international proche du standard *Bell 103*.
Bell 212A	1200 bps	Full duplex	Standard américain et canadien fonctionnant selon le codage à changement de phase différentiel. Il permet de cette façon de transmettre 2 bits par baud
UIT V.22	1200 bps	Half duplex	Standard international proche du standard *Bell 212A*.
UIT V.22bis	2400 bps	Full duplex	Standard international constituant une version améliorée du standard V.22 (d'où l'appellation *V.22bis*).
UIT V.23	1200 bps	Half duplex	Standard international fonctionnant en half-duplex, c'est-à-dire permettant de

			transférer les données sur une seule voie à la fois. Possibilité d'une voie de retour à 75 bauds facultative.
UIT V.23	1200 bps/75 bps	Full duplex	Standard international fournissant un duplex intégral asymétrique, c'est-à-dire qu'il permet de transférer des données à 1200 bps dans un sens et 75 bps dans l'autre.

Tableau 3.01: Exemples de standards de modem

3.3 La liaison Bluetooth

3.3.1 Présentation de la technologie

Bluetooth est une technologie de réseau personnel sans fils, noté WPAN pour Wireless Personal Area Network, c'est-à-dire une technologie de réseaux sans fils d'une faible portée permettant de relier des appareils entre eux sans liaison filaire. Contrairement à la technologie utilisant la liaison infrarouge, les appareils Bluetooth ne nécessitent pas une ligne de vue directe pour communiquer, ce qui rend plus souple son utilisation et permet notamment une communication d'une pièce à une autre, sur de petits espaces.

L'objectif de la technologie Bluetooth est de permettre la transmission des données ou de la voix entre des équipements possédant un circuit radio de faible coût, sur un rayon de l'ordre d'une dizaine de mètres à un peu moins d'une centaine de mètres et avec une faible consommation électrique. [9]

Ainsi, la technologie Bluetooth est principalement prévue pour relier entre eux des périphériques (imprimantes, téléphones portables, appareils domestiques, oreillettes sans fils, souris, clavier, etc.),

des ordinateurs ou des assistants personnels (PDA), sans utiliser une liaison filaire. La technologie Bluetooth est également de plus en plus utilisée dans les téléphones portables, afin de leur permettre de communiquer avec des ordinateurs ou des assistants personnels et surtout avec des dispositifs mains-libres tels que des oreillettes Bluetooth.

3.3.2 Caractéristiques

Une interface Bluetooth est constituée d'une interface radio, d'un contrôleur et d'une interface avec le système hôte.

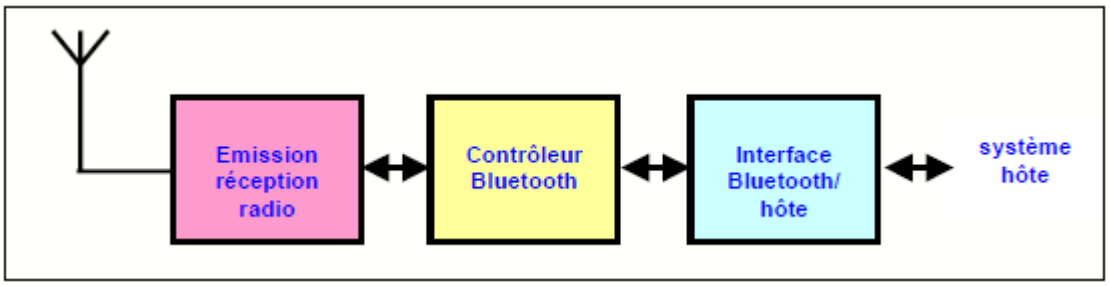

Figure 3.02: Schéma bloc d'une interface Bluetooth

Chaque système (téléphone, PC …) compatible «Bluetooth» est équipé d'une interface identique grâce à laquelle il pourra communiquer avec les autres systèmes compatibles.

La liaison radio fonctionne dans une bande de fréquence située autour de 2,45 GHz libre dans la plupart des pays, ce qui permet d'utiliser les équipements Bluetooth partout dans le monde.

Le Bluetooth permet d'obtenir des débits de l'ordre de 1 Mbps, correspondant à 1600 échanges par seconde en full-duplex, avec une portée d'une dizaine de mètres environ avec un émetteur de classe 2 et d'un peu moins d'une centaine de mètres avec un émetteur de classe 1.

En effet, le standard Bluetooth définit 3 classes d'émetteurs proposant des portées différentes en fonction de leur puissance d'émission :

Classe	Puissance d'émission	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	15-20 mètres
3	1 mW (0 dBm)	10 mètres

Tableau 3.02: Classes d'émetteur

Outre la dépendance vis-à-vis de la puissance émise, la portée de la liaison dépend aussi :

- du gain des antennes : une antenne de bonne qualité permet d'augmenter la portée, mais est difficile à installer à l'intérieur d'un téléphone ou d'un PC portables
- de l'environnement : l'onde radio doit contourner ou traverser plusieurs obstacles qui absorberont une partie de l'énergie émise. Elle peut aussi être diffractée par un obstacle conducteur et renvoyée dans toutes les directions. Enfin, l'arrivée sur l'antenne du récepteur d'ondes ayant suivi des trajets différents peut aussi conduire à des interférences destructives.

Contrairement à la technologie infrarouge, principale technologie concurrente utilisant des rayons lumineux pour la transmission de données, la technologie Bluetooth utilise les ondes radio (bande de fréquence des 2.4 GHz) pour communiquer, si bien que les périphériques ne doivent pas nécessairement être en liaison visuelle pour communiquer. Ainsi deux périphériques peuvent communiquer en étant situés de part et d'autre d'une cloison et les périphériques Bluetooth sont capables de se détecter sans intervention de la part de l'utilisateur pour peu qu'ils soient à portée l'un de l'autre.

3.3.3 Topologie du réseau

Bluetooth est un réseau de type «ad-hoc» c'est-à-dire sans station de base :

- ce réseau est auto-configurable. Deux machines mobiles se retrouvant dans le même secteur peuvent se reconnaître puis échanger des données
- chaque machine peut échanger des informations avec n'importe quelle autre machine
- les nœuds peuvent échanger des données uniquement lorsqu'ils sont à portée de réception l'un par rapport à l'autre.

Dans un réseau Bluetooth, on peut retrouver des « piconet » et des « scatternet ».

Un piconet ou picoréseau est un mini-réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon. Un picoréseau est organisé selon une topologie en étoile : il y a un « maître » et plusieurs « esclaves ». Il est constitué de 8 appareils au maximum avec une adresse codée sur 3 bits.

La communication est directe entre le « maître » et un « esclave ». Les « esclaves » ne peuvent pas communiquer entre eux. Tous les « esclaves » du picoréseau sont synchronisés sur l'horloge du « maître ». C'est le « maître » qui détermine la fréquence de travail pour tout le picoréseau. Les appareils ne faisant pas partie du piconet sont en mode «stand-by» ou «park».

Les périphériques « esclaves » peuvent avoir plusieurs « maîtres » : les différents piconets peuvent donc être reliés entre eux. Le réseau ainsi formé est appelé « réseau de diffusion » ou « scatternet ».

Les figures 3.03 et 3.04 illustrent ces deux types de réseau.

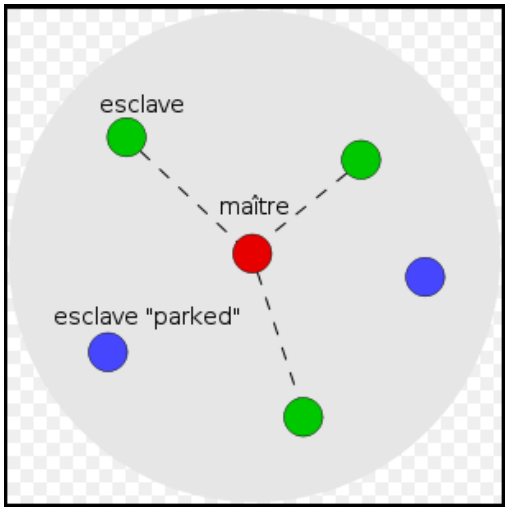

Figure 3.03: Réseau piconet

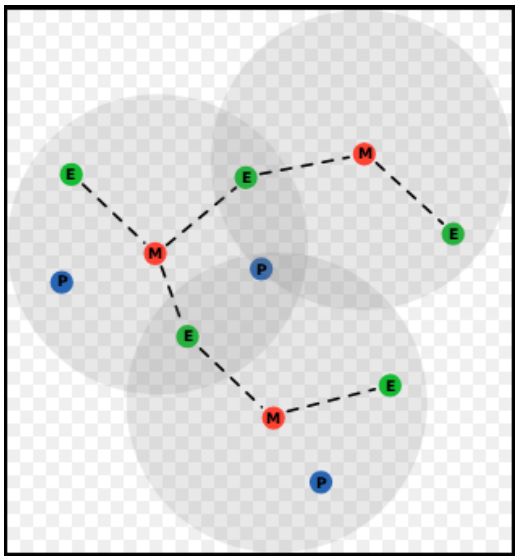

Figure 3.04: Réseau scatternet

3.4 Le réseau Wi-Fi

3.4.1 Présentation générale

Le Wi-Fi, contraction de Wireless Fidelity, est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques comme les ordinateurs, routeur, smartphone, décodeur Internet, au sein d'un réseau informatique afin de permettre la transmission de données entre eux. [10]

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fils à haut débit pour peu que l'ordinateur à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des ordinateurs de bureau, des assistants personnels ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur à plusieurs centaines de mètres en environnement ouvert.

3.4.2 Structure

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques:

- la couche physique (notée parfois couche PHY), proposant quatre types de codage de l'information (DSSS, FHSS, OFDM, Infrarouge)
- la couche liaison de données, constituée de deux sous-couches :
    - le contrôle de la liaison logique (Logical Link Control, ou LLC)
    - le contrôle d'accès au support (Media Access Control, ou MAC)

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations.

La norme 802.11 propose donc en réalité trois couches : une couche physique appelée PHY et deux sous-couches relatives à la couche liaison de données du modèle OSI. Ils définissent des modes de transmission alternatifs. [11]

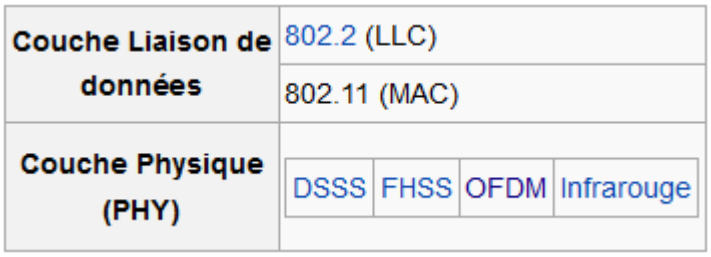

Figure 3.05: Structure et couches du protocole

DSSS: Direct Sequence Spread Spectrum

FHSS: Frequency-Hopping Spread Spectrum

OFDM: Orthogonal Frequency-Division Multiplexing

3.4.3 Modes de mise en réseau

3.4.3.1 Le mode architecture

Le mode Infrastructure est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (PA) qui agissent comme des concentrateurs. La mise en place d'un tel réseau oblige de poser des bornes « Point d'accès » dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau afin de pouvoir communiquer.

L'avantage de ce mode est de garantir un passage obligé par le Point d'accès. Il est donc possible de vérifier qui accède au réseau.

3.4.3.2 Le mode « ad hoc »

Le mode « *Ad-Hoc* » est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire. La mise en place d'un tel réseau ne nécessite qu'une configuration des machines en mode ad hoc.

L’avantage de ce mode est de s’affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de point d'accès.

3.5 Universal Serial Bus

L’Universal Serial Bus, connu sous l’acronyme USB, est une norme relative à un bus informatique en transmission série qui sert à connecter des périphériques informatiques à un ordinateur. Le bus USB permet de connecter des périphériques à chaud et en bénéficiant du Plug and Play, c’est-à-dire que le système reconnaît automatiquement le périphérique. [12]

3.5.1 Fonctionnement du bus USB

L'architecture USB a pour caractéristique de fournir l'alimentation électrique aux périphériques qu'elle relie, dans la limite de 15 W maximum par périphérique. Elle utilise pour cela un câble composé de quatre fils : la masse GND, l'alimentation VBUS et deux fils de données appelés D- et D+. [13]

Figure 3.06: Schéma global des broches du connecteur

La communication entre l'ordinateur et les périphériques se fait selon un protocole basé sur le principe de l'anneau à jeton « Token Ring ». Cela signifie que la bande passante est partagée temporellement entre tous les périphériques connectés. L'ordinateur émet un signal de début de séquence chaque milliseconde, intervalle de temps pendant lequel il va donner simultanément la « parole » à chacun d'entre eux. Lorsque l'ordinateur désire communiquer avec un périphérique, il émet un jeton, c’est-à-dire un paquet de données contenant l'adresse du périphérique, codé sur 7 bits

et désignant un périphérique. C'est donc l'hôte qui décide du « dialogue » avec les périphériques. Si le périphérique reconnaît son adresse dans le jeton, il envoie un paquet de données en réponse, sinon il fait suivre le paquet aux autres périphériques connectés. Les données ainsi échangées sont codées selon le codage NRZI. Puisque l'adresse est codée sur 7 bits, 128 périphériques peuvent être connectés simultanément à un port de ce type. Il convient en réalité de ramener ce chiffre à 127 car l'adresse 0 est une adresse réservée. Les ports USB supportent le **Hot plug and play**. Ainsi, les périphériques peuvent être branchés sans éteindre l'ordinateur. Lors de la connexion du périphérique à l'ordinateur, ce dernier détecte l'ajout du nouvel élément grâce au changement de la tension entre les fils D+ et D-. A ce moment, l'ordinateur envoie un signal d'initialisation au périphérique pendant 10 ms, puis lui fournit du courant grâce aux fils GND et VBUS. Le périphérique est alors alimenté en courant électrique et récupère temporairement l'adresse par défaut correspondant à l'adresse 0. L'étape suivante consiste à lui fournir son adresse définitive par la procédure d'énumération. Pour cela, l'ordinateur interroge les périphériques déjà branchés pour connaître la leur et en attribue une au nouveau, qui en retour s'identifie. L'ordinateur, disposant de toutes les caractéristiques nécessaires, est alors en mesure de charger le pilote approprié.

3.5.2 Evolution de la norme USB

L'USB a été conçu au milieu des années 1990 afin de remplacer les nombreux ports externes d'ordinateurs, lents et incompatibles les uns avec les autres. Différentes versions de la norme ont été développées au fur et à mesure des avancées technologiques, chacune étant vouée à remplacer les précédentes car plus performante.

3.5.2.1 USB 1

La première version de la norme, l'USB 1.0, est spécifiée par sept partenaires industriels (Compaq, DEC, IBM, Intel, Microsoft, NEC et Northern Telecom). Mais elle reste théorique et n'a jamais vraiment été appliquée. Par manque de composants, il faudra attendre la seconde version de la norme en 1998, intitulée USB 1.1, pour que l'USB commence à être effectivement utilisé.

L'USB 1.1 apporte des corrections à la norme 1.0 et définit également deux vitesses de communication :

- le *mode lent (Low Speed)* a un débit de 190 Ko/s. Il permet de connecter des périphériques qui ont besoin de transférer peu de données, comme les claviers et souris
- le *mode pleine vitesse (Full Speed)* débite à 1,5 Mo/s. Il est utilisé pour connecter des imprimantes, scanners, disques durs, graveurs de CD et autres périphériques ayant besoin de plus de rapidité. Néanmoins, il est insuffisant pour beaucoup de périphériques de stockage de masse.

3.5.2.2 USB 2

En avril 2000 est publiée la norme USB 2.0, qui optimise l'utilisation de la bande passante et surtout introduit un troisième débit à **60 Mo/s**, baptisé Haute vitesse ou High Speed. Il est utilisé par les périphériques rapides tels que les disques durs, graveurs et autres périphériques.

En 2005, le Wireless USB, une version sans-fil de l'USB, fait son apparition. Elle promet 50 Mo/s à une distance de 3 m et 14 Mo/s à 10 m.

L'extension On-The-Go (OTG), ajoutée à la norme USB 2.0 en 2007, permet d'effectuer des échanges de données point à point entre deux périphériques sans avoir à passer par un hôte. La norme OTG s'impose désormais comme un standard.

3.5.2.3 USB 3

En 2008, l'USB 3.0 introduit le mode vitesse supérieure ou SuperSpeed, qui débite théoriquement à 625 Mo/s. Mais la vitesse de transfert réelle est seulement de 500 Mo/s. L'USB 3 délivre une puissance électrique de 4,5 watts.

Les nouveaux périphériques disposent de connexions à 6 contacts au lieu de 4, mais la compatibilité ascendante des prises et câbles avec les versions précédentes est assurée. En revanche, la compatibilité descendante est impossible, les câbles USB 3.0 n'étant pas compatibles avec les prises USB 1.1 ou USB 2.0. Cependant il existe des adaptateurs.

3.6 Le réseau GSM

Le réseau GSM est l'un des facteurs dominants dans le domaine de la télécommunication. En effet, les avantages qu'il offre ainsi que son mode de fonctionnement joue en sa faveur. [14]

3.6.1 Architecture d'un réseau GSM

3.6.1.1 Station mobile

La station mobile est un terminal mobile authentifié et autorisé à accéder au réseau mobile. Elle est caractérisée par l'association de deux éléments principaux :

- Le terminal physique, appelé Mobile Equipment, habituellement représenté par un téléphone mobile
- Une carte SIM (Subscriber Identity Module) représentant l'abonnement souscrit et contenant les paramètres clés le concernant

L'utilité de la séparation de ces deux éléments se focalise surtout sur le fait qu'on puisse utiliser le même terminal physique avec différents abonnements ainsi qu'un abonnement avec plusieurs terminaux. [15]

3.6.1.2 Station de base

La station de base ou BTS (Base Transceiver Station) constitue un des éléments de base du système de téléphonie mobile GSM.

Dans un réseau GSM, le territoire est découpé en petites zones appelées cellules dont la superficie varie grandement suivant la localisation de la zone étudiée. Généralement, dans les zones urbaines, la taille des cellules est réduite et, au contraire, dans les zones rurales, elle est beaucoup plus grande. Une station de base est caractérisée par deux grands points : le type d'antenne et la taille de la cellule. On distingue, entre autres, des antennes omnidirectionnelles émettant à 360°, des antennes bidirectionnelles émettant à 180° ainsi que des antennes tri-sectorielles dont chacune des antennes assure 120°. Ce dernier type d'antenne est la plus utilisée étant donné qu'elle optimise la communication et limite les interférences. [15]

Une station de base assure la liaison radio avec les stations mobiles. Ces principaux rôles sont :

- L’activation et la désactivation d’un canal radio
- Le multiplexage temporel et la gestion des sauts de fréquence
- La sécurisation du contenu à transmettre par chiffrement
- La surveillance et la sécurisation de la communication
- Le contrôle de la liaison
- La surveillance des niveaux de champ reçu et de la qualité des signaux
- Le contrôle de la puissance d'émission

3.6.1.3 Base Station Controller

Le BSC ou Base Station Controller assure le rôle de commander un certain nombre de stations de base. Il est chargé de gérer la partie intelligente de la communication, c’est-à-dire qu’il décide de l’activation ou de la désactivation d’un canal vers une station mobile ainsi que de la puissance d’émission d’une station de base, il gère aussi le changement de cellules et la synchronisation de l’heure des stations de base. [15]

3.6.1.4 Mobile Switching Center

Le MSC ou Mobile Switching Center est un équipement de téléphonie mobile chargée du routage dans le réseau, de l’interconnexion avec les autres réseaux et de la coordination des appels. De même que chaque BSC concentre le trafic de plusieurs BTS, le MSC concentre les flux de données en provenance de plusieurs BSC. Il est aussi à noter qu’un VLR est associé à un MSC. Ce VLR connait les informations détaillées sur les usagers que le MSC doit gérer. Le MSC assure alors l’interconnexion des abonnées du réseau GSM et l’interconnexion du réseau avec les autres réseaux. Ses principaux rôles sont :

- La commutation étant donné que le MSC est un centre de routage et de multiplexage
- La gestion des connexions
- La localisation et la détermination de l’itinérance
- Le contrôle du handover entre deux BSC dont il a la charge
- La gestion des handover d’une station mobile quittant son domaine d'influence vers celui d'un autre MSC.

3.6.1.5 Home Location Register

Il s'agit de la base de données centrale d'un opérateur de réseau mobile, comportant les informations relatives à tout abonné autorisé à utiliser ce réseau et notamment sa localisation dans le réseau. Ces informations sont divisées en deux grandes parties : les informations statiques et les informations dynamiques. Les informations statiques font références aux détails des options souscrites et des services supplémentaires accessibles à l'abonnée. Les informations dynamiques concernent les informations telles que la dernière localisation connue de l'abonné et l'état de son terminal (en service, hors service, en communication, en veille). Ces informations sont actualisées en permanence. L'utilité de ces informations dynamiques apparait surtout lorsque le réseau achemine un appel vers l'abonné. Il commence tout d'abord par interroger son HLR pour prendre connaissance de la dernière localisation connue de l'abonné, du dernier état de son terminal avant toutes actions. Le HLR contient également une clé secrète de chaque abonné permettant au réseau de certifier son identité.

3.6.1.6 Visitor Location Register

Le VLR est une base de données temporaire contenant des informations sur tous les utilisateurs d'un réseau, et qui est parfois intégré dans le Mobile service Switching Center (MSC). Sa mission consiste à enregistrer les informations dynamiques relatives aux abonnés de passage dans le réseau. Cette gestion effectuée par le VLR permet de connaître la localisation de tous les abonnés présents, c'est-à-dire de savoir dans quelle cellule se trouve chacun d'eux. Effectivement, la spécificité des abonnés d'un réseau GSM étant la mobilité, il faut en permanence localiser tous les abonnés présents dans le réseau et suivre leurs déplacements. A chaque changement de cellules d'un abonné, le réseau doit mettre à jour le VLR du nouveau réseau visité et le HLR de l'abonné.

3.6.1.7 Authentification Center

Le centre d'authentification ou AUC est une base de données qui stocke des informations confidentielles. Il désigne une fonction d'authentification via la carte SIM des téléphones mobiles utilisés sur un réseau mobile GSM. Le centre d'authentification contrôle les droits d'usages possédés par chacun des abonnés sur les services du réseau et vérifie les identités des abonnés. Cette authentification a lieu normalement après la mise sous tension du téléphone mobile. Et aussitôt que

la carte SIM est authentifiée, le HLR est en mesure d'administrer la carte SIM et les services de téléphonie mobile associés.

L'AUC a été mis en place pour que l'opérateur s'assure que, lorsqu'un abonné passe une communication, il ne s'agit pas d'un usurpateur. Il remplit alors une fonction de protection de la communication qui se fait en deux mécanismes :

- Le chiffrement radio
- L'authentification des utilisateurs du réseau au moyen d'une clé K, qui est à la fois présente dans la station mobile et dans le centre d'authentification.

On peut ainsi obtenir trois niveaux de protection :

- La carte SIM qui interdit à un utilisateur non enregistré d'avoir accès au réseau.
- Le chiffrement des communications destiné à empêcher l'écoute de celles-ci.
- La protection de l'identité de l'abonné

3.6.2 Les interfaces

Les interfaces sont des composantes importantes du réseau car elles assurent le dialogue entre les équipements et permettent leur interfonctionnement.

3.6.2.1 L'interface radio Um

Cette interface se localise entre la station mobile et la station de base. Elle est la plus importante interface du réseau.

3.6.2.2 L'interface A-bis

Elle constitue l'interface entre la station de base et son BSC.

3.6.2.3 L'interface A

C'est l'interface entre un BSC et un commutateur.

3.6.2.4 L'interface X25

Cette interface se situe entre un BSC et le centre d'exploitation et de maintenance.

3.6.3 Acheminement d'un appel

3.6.3.1 Mise sous tension

Le fonctionnement suit les étapes suivantes :

- l'utilisateur valide sa carte SIM en tapant au clavier son numéro de code PIN
- le récepteur du GSM scrute les canaux de la bande GSM et mesure le niveau reçu
- le mobile repère la voie balise de niveau le plus élevé correspondant à son opérateur
- le mobile récupère le signal de synchronisation de la trame TDMA diffusé sur le BCCH (Broadcast Control Channel) et synchronise sa trame
- le mobile lit sur le BCCH les infos concernant la cellule et le réseau et transmet à la BTS l'identification de l'appelant pour la mise à jour de la localisation.

3.6.3.2 Mode veille

Dans ce mode, le mobile effectue un certain nombre d'opérations de routine :

- lecture du Paging Channel qui indique un appel éventuel
- lecture des canaux de signalisation des cellules voisines
- mesure du niveau des voies balisées (BCH) des cellules voisines pour la mise en route éventuelle d'une procédure de hand-over

3.6.3.3 Réception d'un appel

A la réception d'un appel :

- l'abonné filaire compose le numéro de l'abonné mobile
- l'appel est aiguillé sur le MSC le plus proche
- le MSC le plus proche du mobile fait diffuser dans la zone de localisation, couvrant plusieurs cellules, un message à l'attention du mobile demandé
- le mobile concerné émet des données sur RACH (Random Access Channel)

- le réseau autorise l’accès par le AGCH (Access Grant Channel) et affecte au mobile une fréquence et un time-slot
- l’appelé est identifié grâce à la carte SIM
- le mobile reçoit la commande de sonnerie
- décrochage de l’abonné et établissement de la communication

3.6.3.4 Emission d’un appel

Elle se fait aussi en plusieurs étapes :

- l’abonné mobile compose le numéro du correspondant du réseau téléphonique commuté
- la demande arrive à la BTS de sa cellule par le Random Access Channel
- elle traverse le BSC pour aboutir dans le commutateur du réseau
- l’appelant est identifié et son droit d’usage est vérifié
- l’appel est transmis vers le réseau public
- le BSC demande l’allocation d’un canal pour la future communication
- décrochage du correspondant et établissement de la communication

3.6.4 Short Message Service

Le service de messagerie SMS est un des services de la téléphonie mobile. Le service de messages courts SMS encore appelé "texto", s’appuie sur la capacité d’un terminal mobile à émettre ou recevoir des messages alphanumériques. [16]

3.6.4.1 Détails techniques

Les messages courts sont des messages textuels d'au plus 160 caractères et sont délivrés en quelques secondes lorsque le destinataire est rattaché au réseau, même lorsque ce destinataire est en communication. Pour mettre en place ce service de messages courts, l'opérateur doit prévoir un ou plusieurs serveurs dédiés et reliés au réseau. On appelle ce serveur le Short Message Service Center (SMSC). Son rôle est de récupérer les messages envoyés afin de les redistribuer aux destinataires lorsque ceux-ci sont connectés au réseau. Dans le cas contraire, il stocke ces messages. Lorsque le mobile du destinataire peut être de nouveau localisé, le réseau notifie le SMSC qui est alors en

mesure de relayer le message. Le SMSC utilise les services du MSC auquel est rattaché le destinataire pour transmettre un message à un mobile. La livraison du message court est donc garantie même lorsque le terminal mobile est indisponible grâce à la fonction store-and-forward du SMSC. A l'arrivée d'un message SMS, l'usager est averti par un signal sonore, par une icône ou par la notification MESSAGE sur son téléphone mobile. Et à l'aide du menu de son téléphone mobile, l'usager peut alors consulter le message court reçu. Il est à noter que lors de la première utilisation du service SMS, le numéro de SMSC doit être mémorisé dans le téléphone mobile.

3.6.4.2 Classe des SMS

Un SMS reçu sur le mobile est traité de manière différente suivant sa classe. La classe est définie dans le SMS Data Coding Scheme :

- classe 0 : appelé encore flash SMS, le message est directement affiché à l'utilisateur sur l'écran du mobile à la réception. Un rapport est envoyé ensuite au centre de service. Le message n'est enregistré ni dans la mémoire du téléphone ni dans la carte SIM. Il est effacé dès que l'utilisateur a validé la visualisation.
- classe 1 : le message est enregistré dans la mémoire du téléphone et si cette mémoire est pleine, dans la carte SIM par défaut.

3.7 Conclusion

Les différents matériels et techniques présentés montrent que toutes liaisons avec l'hôte, ici représenté par un ordinateur, sont permises tant que ce dernier reconnait les périphériques. De nos jours, les avancées technologiques ne cessent de s'accroître. La qualité ainsi que le débit de transfert des données s'améliorent de jour en jour. L'application ne se limite pas à un seul type de connexion liant l'ordinateur avec les périphériques mais s'adapte facilement à l'évolution technologique. Et l'utilisation de ces nouvelles générations de technologie élargit considérablement le champ d'action et l'efficacité de l'application.

CHAPITRE 4

REALISATION

4.1 Introduction

Dans ce dernier chapitre, le mode d'utilisation ainsi que le mode de fonctionnement de l'application seront mis en relief. Ainsi, les différents utilisateurs de l'application peuvent se référer et connaître les procédés pour la mise en marche du programme. Dans cette partie, les explications seront surtout orientées pratiques.

4.2 Description

4.2.1 Position du problème

La sécurisation est l'un des atouts majeurs recherchés par l'homme. En effet, de nos jours, divers problèmes surviennent dans la vie quotidienne, et qui sont notamment dominés par le vol et les effractions. Nous nous faisons déposséder de nos biens avant même que nous nous en rendions compte.

Ce projet consiste justement à minimiser les probabilités d'occurrence de ces faits par le biais d'un système de sécurisation implémenté à l'aide d'une application.

Sur le plan matériel, cette application fait appel à trois composants de base : un téléphone portable pouvant être utilisé en tant que modem, un ordinateur et une webcam.

4.2.2 Description du système

La figure 4.01 montre le principe du montage :

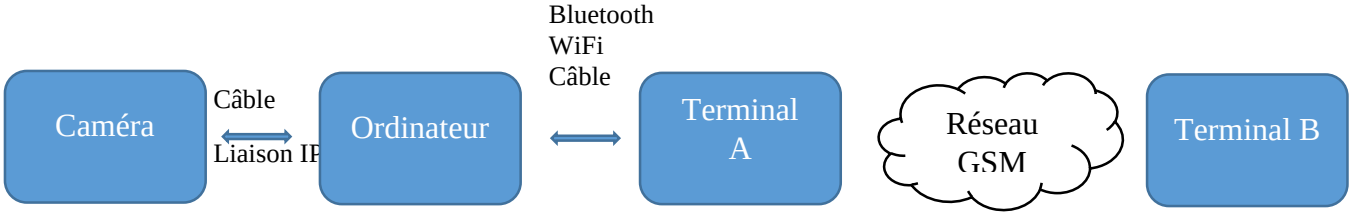

Figure 4.01 : Schéma bloc du système

- Différents types de caméras peuvent s'adapter au système, que ce soit une caméra IP, fonctionnant à travers une adresse IP, ou une caméra analogique liée à l'ordinateur par l'intermédiaire d'un câble USB
- L'ordinateur, lui, constitue le cœur du système, c'est celui qui assure son bon fonctionnement. En effet, c'est sur ce dernier que l'application est installée. Cela lui permet la gestion de tous les périphériques qui lui sont connectés.
- Le terminal A est représenté par un téléphone assurant le rôle de modem. Divers types de connexion peuvent être établis : connexion par câble USB, connexion par WiFi, ou connexion Bluetooth.

  Ces 3 premiers blocs se situent au niveau du local à surveiller.
- Le terminal B, quant à lui, se situe dans un autre endroit. Il est aussi représenté par un téléphone sur lequel seront envoyées les informations obtenues par l'ordinateur.

  Il est à noter que le terminal A et le terminal B communique à travers le réseau GSM.

4.2.3 Principe de fonctionnement et structure

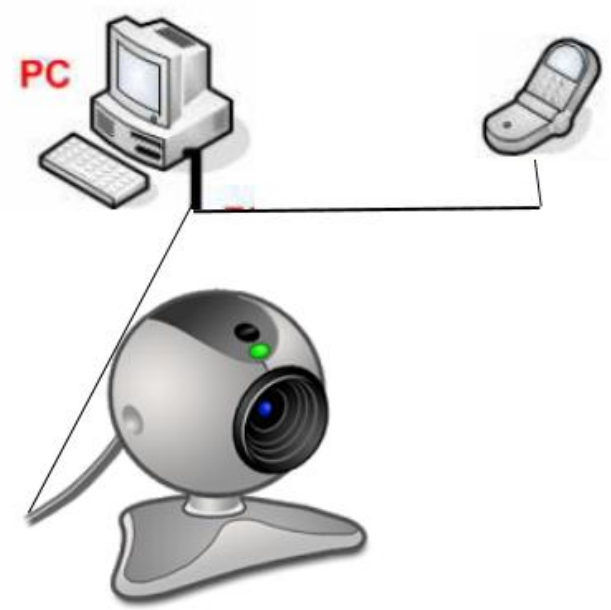

Figure 4.02 : Structure de base

L’application fait appel à 3 composants interagissant entre eux : un ordinateur, une webcam et un téléphone portable. Et elle tourne au niveau de l’ordinateur. Avant de définir plus précisément le déroulement de ce projet, il est nécessaire de savoir que tous les phénomènes qui suivent sont supposés se dérouler dans un endroit démuni de présence, mais toutefois les autres cas ont aussi leurs places. Dans le premier cas, après activation de la sécurisation intelligente, aux moindres mouvements suspects, la webcam envoie un signal vers l’ordinateur en lui indiquant qu’un évènement à risque potentiel est survenu. L’ordinateur, lui, traduit cette information en tant qu’approbation afin de permettre au téléphone de mettre au courant l’hôte du site concerné soit par l’intermédiaire d’un message texte, soit par appel ou même les deux suivant les préférences de l’utilisateur.

4.3 Objectifs

Ce système de vidéosurveillance a deux fonctions principales :

- La dissuasion :

En effet, les systèmes de vidéosurveillance sont dissuasifs car ils sont généralement visibles de tous. Et cela constitue une manière efficace pour toutes sortes de vols, intrusions et dégradations.

- La surveillance :

Outre le phénomène de dissuasion, ce système de surveillance peut aussi bien être discret que voyant. Le résultat recherché étant le même c’est-à-dire surveiller une zone où le risque et la menace sont présents.

L’objectif est donc de contribuer à la sécurité de biens ou de personnes.

Cette contribution concerne divers faits, souvent imbriqués.

4.3.1 Prévention de la criminalité

La vidéosurveillance représente une arme innovante et efficace dans la lutte contre la criminalité et les atteintes à l’ordre public. Elle offre ainsi la possibilité de mieux maîtriser l’environnement et les flux d’informations. Les systèmes de vidéosurveillance permettent parfois de détecter les signes

avant-coureurs d'infractions pénales mais ils peuvent également servir d'outils de réaction. La vidéosurveillance permet effectivement d'observer les faits et gestes collectifs ou individuels, d'anticiper les menaces et donc d'informer son ou ses utilisateurs des comportements et actes nuisibles avant, pendant et après un évènement donné. Comme exemple concret, elle a contribué à l'identification des attentats à la bombe qui ont frappé les quartiers londoniens de Bishopsgate en 1994 et divers points du capital britannique le 7 juillet 2005.

4.3.2 Sécurité routière

Dans le domaine de la sécurité routière, la vidéosurveillance a permis de lever les angles morts. Dans cette approche, le chauffeur peut voir les mouvements des employés à l'arrière de son véhicule. Les caméras de surveillance embarquées, utilisées dans les véhicules de police, permettent de scanner les plaques minéralogiques. Les chiffres ainsi obtenus peuvent ensuite être comparés à une base de données maîtresse dans laquelle figurent tous les véhicules immatriculés, afin d'établir les correspondances en cas de vol de voiture ou d'autres infractions. Et il est aussi à noter que la vidéosurveillance se développe pour l'accès en temps réel de la circulation routière des voies les plus fréquentées ainsi que pour la détection d'accident.

4.3.3 Sécurité industrielle

Les sites de production sont équipés de systèmes de *vidéosurveillance* permettant notamment de multiplier les points d'observation en temps réel de l'état des installations et du déroulement du procédé.

En plus de tous ces objectifs, la vidéosurveillance permet aussi de surveiller divers lieux pour prévenir les intrusions et les dégradations venant de personnes malveillantes. Tout cela dans le but d'améliorer nettement la sûreté.

4.4 Présentation de la réalisation

4.4.1 Choix du langage

Java est un langage de programmation moderne très utilisé dans le monde. Il est surtout renommé pour sa portabilité ; en effet, c'est un langage de programmation informatique orienté objet dont la particularité et l'objectif central sont de faciliter le fonctionnement d'un même logiciel sur différents systèmes d'exploitation.
La programmation orientée objet consiste à faire interagir plusieurs briques de logiciels appelées objet. Un objet peut être défini comme étant une structure de données cachées et munies de valeur, et qui répond à un ensemble de messages. Il est surtout caractérisé par des attributs et des méthodes lui permettant d'interagir avec d'autres objets.

Java est normalement utilisée pour développer des applications graphiques. Il est à noter que le logiciel ayant permis la conception de ce travail est Eclipse IDE (Integrated Development Environment). Eclipse IDE est un environnement de développement libre codé en java et dont l'architecture est totalement développée autour de la notion de plug-in, c'est-à-dire que si nous voulons ajouter de nouvelles fonctionnalités à Eclipse, nous devons télécharger le plug-in correspondant, copier les fichiers spécifiés dans les répertoires spécifiés et démarrer Eclipse. Pour pouvoir l'utiliser, il est impératif d'avoir un environnement java ou JRE (Java Runtime Environment) sur la machine. Un JRE permet la lecture des programmes qui ont été codés en java. Effectivement, dans ce JRE se trouve le cœur de java : le JVM (Java Virtual Machine). C'est cette dernière qui permet l'exécution des programmes java sur votre machine. C'est-à-dire qu'avant d'être utilisés par la machine virtuelle, les programmes java sont précompilés en byte code par votre IDE. Et c'est à partir de ce byte code que le JVM arrive à comprendre le programme permettant d'effectuer le lien entre le code et votre machine.

4.4.2 Interface graphique

L'interface graphique comporte des onglets, des fenêtres, des boutons et des listes déroulantes. La figure 4.03 montre le premier aperçu au lancement de l'application.

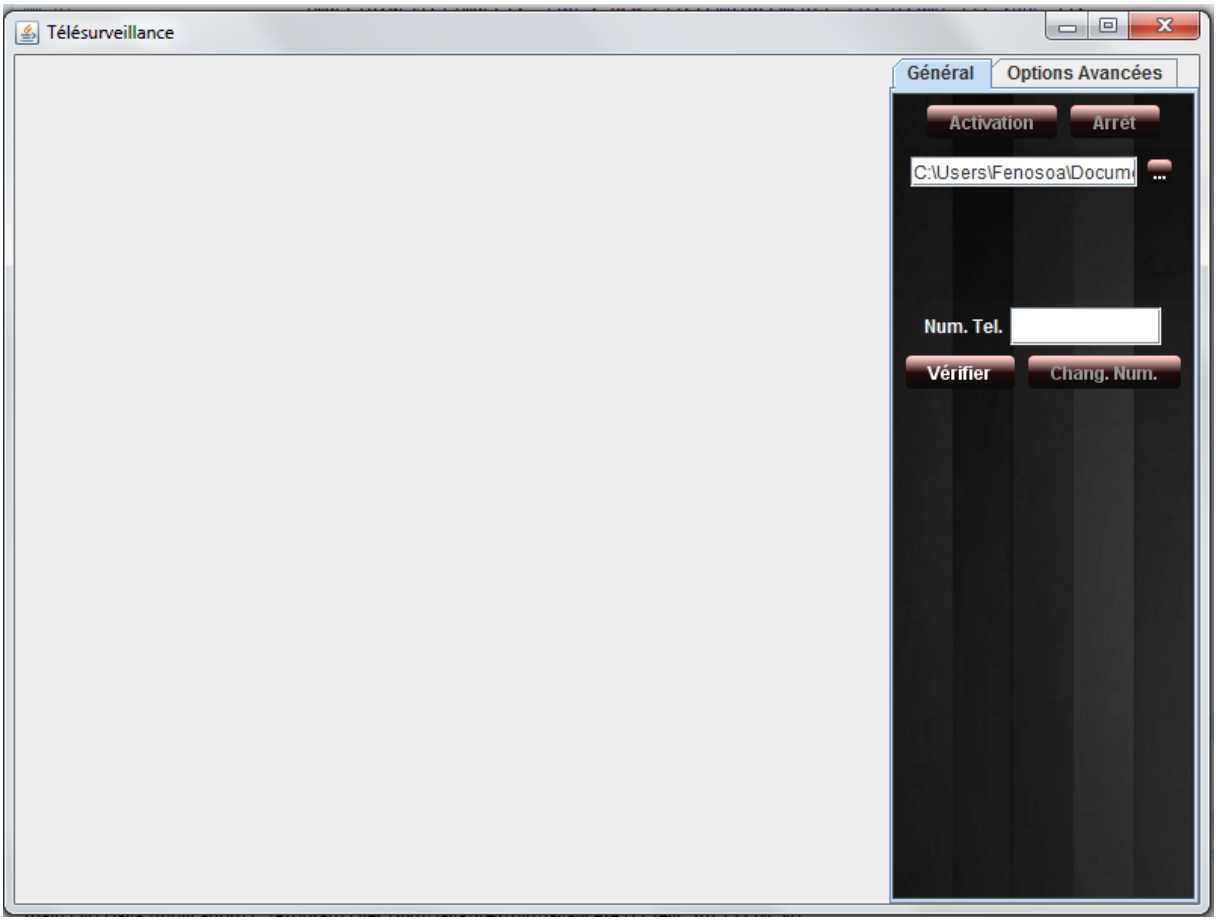

Figure 4.03: Premier aperçu de l'interface graphique

4.4.3 Configuration matérielle

Les matériels fondamentaux permettant le fonctionnement de l'application sont : l'ordinateur, un téléphone portable et une caméra.

L'application accepte de larges gammes de caméras y compris les cameras USB ainsi que les cameras IP, du moment que celles-ci soient reconnues par l'application. Le téléphone, quant à lui, peut être connecté à l'ordinateur de diverses manières :

- par liaison Bluetooth
- en utilisant le Wi-Fi
- ou par câble USB

Le but recherché, ici, étant de pouvoir utiliser le téléphone en tant que modem. Une fois qu'il est reconnu en tant que modem, l'ordinateur lui alloue un port de communication qui sera utile pour le

bon fonctionnement de l'application. Dans Windows, ce port est connu en suivant la méthode suivante :

Panneau de configuration >> Téléphone et modem >> Modems

Cette méthode permet d'accéder à l'utilitaire qui indiquera les différents ports utilisés.

4.4.4 Configuration de l'application

Cette application offre une interface graphique, qui se veut être très simple à manipuler, permettant ainsi de cibler tout genre de personnes ayant ou non une connaissance avancée en informatique.

4.4.4.1 L'onglet « Général »

Cet onglet est affiché dès le démarrage de l'application. Il présente les configurations de base pour mettre l'application en marche. Dans l'onglet général, on retrouve alors les interactions de base. La caméra et le modem, étant connectés au préalable, avant de pouvoir lancer la surveillance, l'utilisateur est invité à entrer le numéro du téléphone à joindre en cas d'alerte. Un champ réservé à cette utilisation est visible dans l'onglet « Général ».

Figure 4.04: *Champ pour le numéro de téléphone*

Afin d'éviter toutes erreurs, comme l'ajout de numéro erroné ou de caractères alphabétiques, un système de contrôle de données à base de regex ou expressions régulières a été implémenté dans ce champ. Ce système permet, entre autres, d'empêcher l'utilisateur d'entrer des données invalides pouvant nuire au bon fonctionnement de l'application.

Après la saisie du numéro de téléphone, l'utilisateur doit vérifier ce numéro par l'intermédiaire du bouton « Vérifier » pour pouvoir continuer. Ce bouton est représenté par la figure 4.05 à la page suivante.

Figure 4.05: *Schéma des boutons de contrôle du numéro de téléphone*

Si tout s'est bien déroulé, l'application renvoie un message affirmant que le numéro a bien été enregistré.

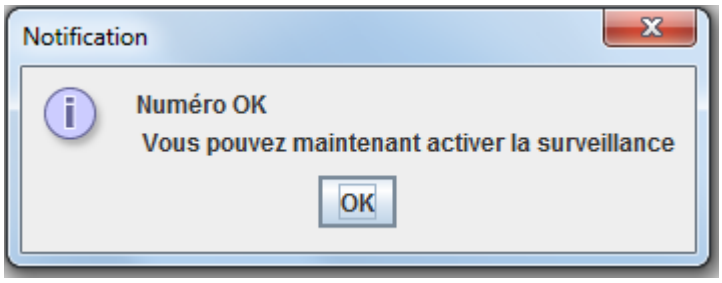

Figure 4.06: *Schéma de la vérification avec succès*

Sinon, si un problème a été détecté par l'application, un message d'erreur apparaît et l'utilisateur doit à nouveau entrer un numéro.

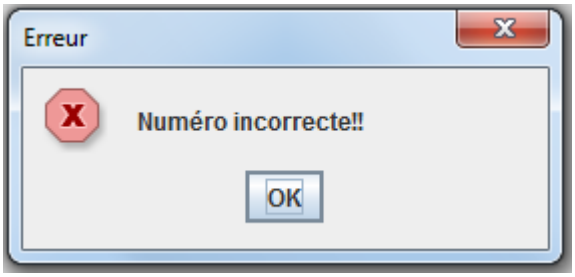

Figure 4.07: *Schéma de détection d'erreur après vérification*

Dans un second lieu, en plus de l'alerte par l'intermédiaire d'un message et d'un appel, cette application capture aussi, en image, tous les évènements ayant déclenché l'alerte. Le répertoire d'enregistrement de ces images, représenté par la figure 4.08, peut être modifié par l'utilisateur. Par défaut, ce répertoire est localisé dans les documents personnels de l'utilisateur.

Figure 4.08: Schéma du répertoire d'enregistrement

En effet, cela permet d'identifier, en cas de fuite, l'individu ayant commis le délit.

Il est à noter que l'utilisateur n'est pas limité à des emplacements locaux mais il peut enregistrer ces images dans une autre machine connectée sur le même réseau.

En se basant sur le fait que l'utilisateur ait saisi un numéro correct, le bouton « Activer » de l'application devient actif et l'utilisateur peut commencer la surveillance.

Figure 4.09: Schéma du bouton d'activation

4.4.4.2 L'onglet « Options Avancées »

La figure 4.10 à la page suivante montre l'interface de l'onglet « Options Avancées ».

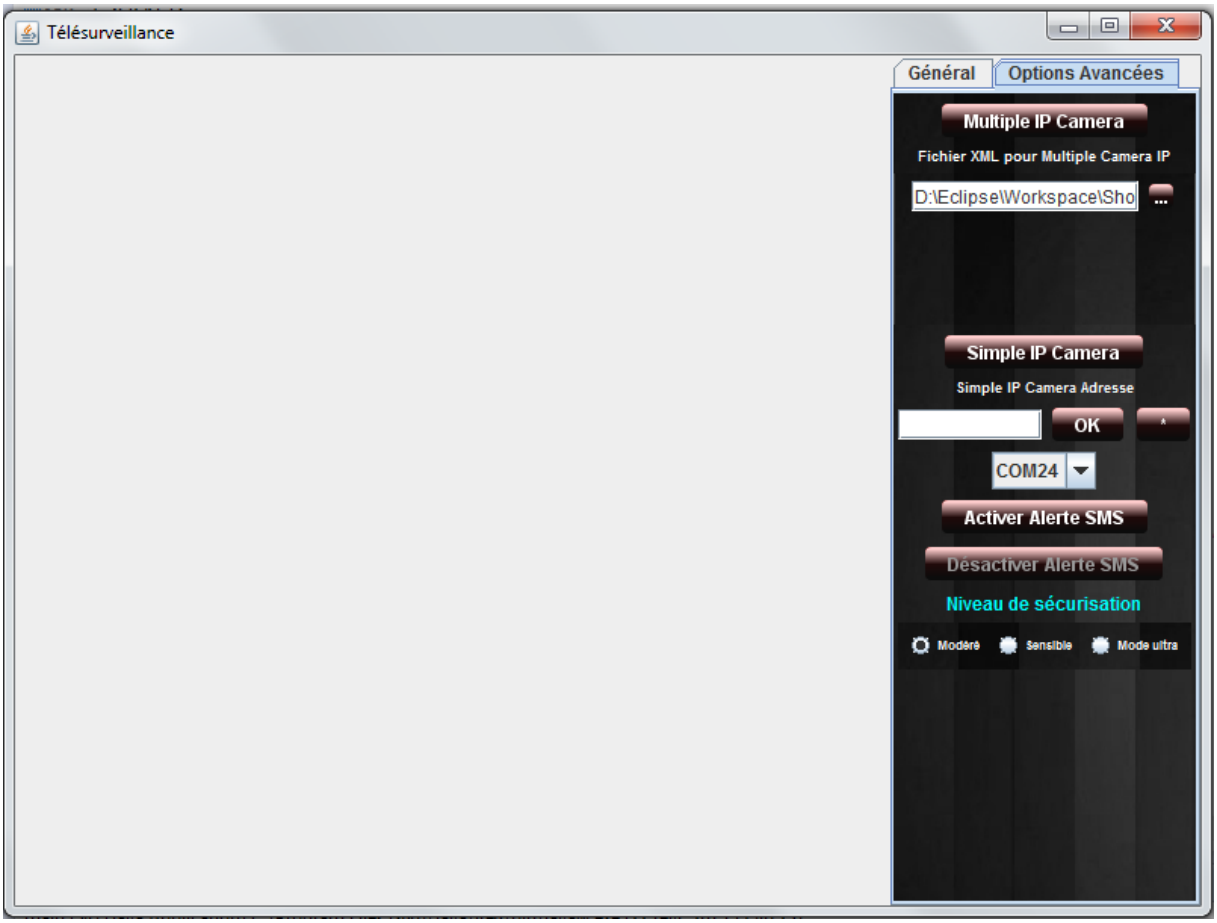

Figure 4.10: Schéma présentant l'onglet "Options Avancées"

Cette interface présente trois grandes parties de configuration :

- configuration de la camera IP
- configuration du modem
- configuration de la sécurisation

L'utilisation des caméras IP nécessite des réglages au préalable. En effet, pour cette configuration, deux choix ayant leurs propres avantages s'offrent à l'utilisateur.

En premier lieu, l'utilisateur peut choisir d'utiliser, en même temps, plusieurs caméras de surveillance en mode « snapshot », c'est-à-dire que ces caméras travaillent en mode photo ; l'acquisition d'image n'est pas continue, elle est espacée par un intervalle de temps défini par un algorithme. Ainsi, tout ce dont l'utilisateur a besoin est l'adresse de chaque caméra qu'il utilisera, le nombre de caméra étant autorisée allant jusqu'à six. Ces adresses sont à insérer dans un

fichier « XML ». Un champ visible dans l'onglet « Options Avancées » permet de récupérer le fichier XML contenant les informations citées ci-dessus.

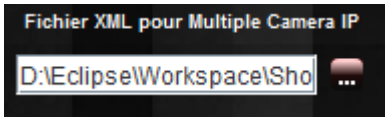

Figure 4.11: Répertoire du fichier XML

```
<?xml version="1.0" encoding="UTF-8" ?>
<storage>
    <ipcam name="Cam 01" url="http://www.dasding.de/ext/webcam/webcam770.php?cam=1" />
    <ipcam name="Cam 02" url="http://www.dasding.de/ext/webcam/webcam770.php?cam=2" />
    <ipcam name="Cam 04" url="http://www.dasding.de/ext/webcam/webcam770.php?cam=4" />
</storage>
```

Figure 4.12: Exemple de fichier XML

Une fois le fichier XML spécifié, l'utilisateur peut activer les caméras en utilisant le bouton « Multiple IP Camera ».

Figure 4.13: Bouton d'activation de plusieurs caméras

Le second choix s'offrant à l'utilisateur est l'utilisation d'une caméra en mode « streaming », c'est-à-dire que l'acquisition d'images se fait de façon continue. Comme pour le cas précédent, l'utilisateur doit se munir de l'adresse IP de la caméra en question suivi du numéro de port. La syntaxe est la suivante « adresse IP : numéro de port ». Lorsque cette adresse a été fournie, l'utilisateur la confirme par l'intermédiaire du bouton « OK » et peut activer la caméra. Un second moyen permet l'utilisation d'une adresse personnalisée. Ainsi, l'utilisateur peut ajouter, lui-même, l'URL et le mode d'accès permettant d'utiliser la caméra. Pour cela, au lieu de confirmer l'adresse à l'aide du bouton « OK », il doit plutôt utiliser le bouton « * ». Les figures 4.14 et 4.15 schématisent ces boutons.

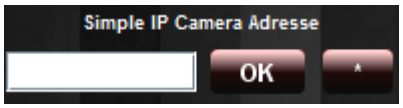

Figure 4.14: Configuration de l'adresse IP de la caméra

Figure 4.15: Bouton d'activation de la caméra

Ensuite, vient une liste déroulante permettant de sélectionner le port sur lequel le modem utilisé est actif. Une fois que le modem est reconnu par l'ordinateur, cette liste se met automatiquement à jour ce qui facilite la tâche de l'utilisateur.

Figure 4.16: Paramétrage du port modem utilisé

Les réglages suivants concernent l'activation ou la désactivation des alertes SMS. Grâce à ces paramètres, l'utilisateur peut être informé par l'intermédiaire d'un SMS de la présence d'un danger de premier niveau. Ainsi, si un danger est capté par la caméra, une alerte de premier niveau est envoyée vers l'utilisateur par le biais d'un SMS. Puis, un appel confirmera que l'alerte est effectivement un danger imminent.

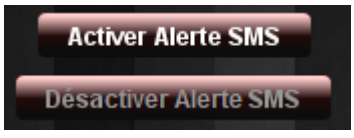

Figure 4.17: Activation/Désactivation de l'alerte SMS

La dernière configuration concerne le niveau de sécurisation. Elle met, à la disposition de l'utilisateur, trois choix parmi lesquels on trouve :

- le niveau « Modéré »
- le niveau « Sensible »
- le niveau « Mode Ultra »

Suivant ces choix proposés, le niveau de perception de la caméra augmente et réagit au moindre mouvement.

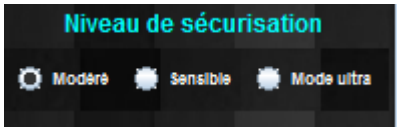

Figure 4.18: Paramétrage du niveau de sécurisation

4.5 Réalisation pratique

Dans cette pratique nous allons utiliser quatre matériels ayant des rôles bien précis :

- un ordinateur de marque « Samsung » sur lequel tournera l'application
- un téléphone « Samsung Galaxy S» qui jouera le rôle de caméra IP
- un téléphone « Nokia Asha 306 » utilisé en tant que modem
- un téléphone « Alcatel » qui recevra les alertes

Ces différents matériels sont illustrés par la figure 4.19.

Figure 4.19: Matériels utilisés

4.5.1 Configurations

Des informations sont nécessaires pour démarrer la sécurisation.

En premier lieu, nous allons configurer le modem. Dans cet exemple, la liaison établie entre l'ordinateur et le téléphone « Nokia » est une liaison Bluetooth. Grâce à l'utilisation du logiciel de Nokia dénommé « Nokia PC-Suite », ce téléphone peut être reconnu par l'ordinateur en tant que modem. Une fois cette étape effectuée, on récupère le port de communication utilisé par le modem comme le montre la figure 4.20.

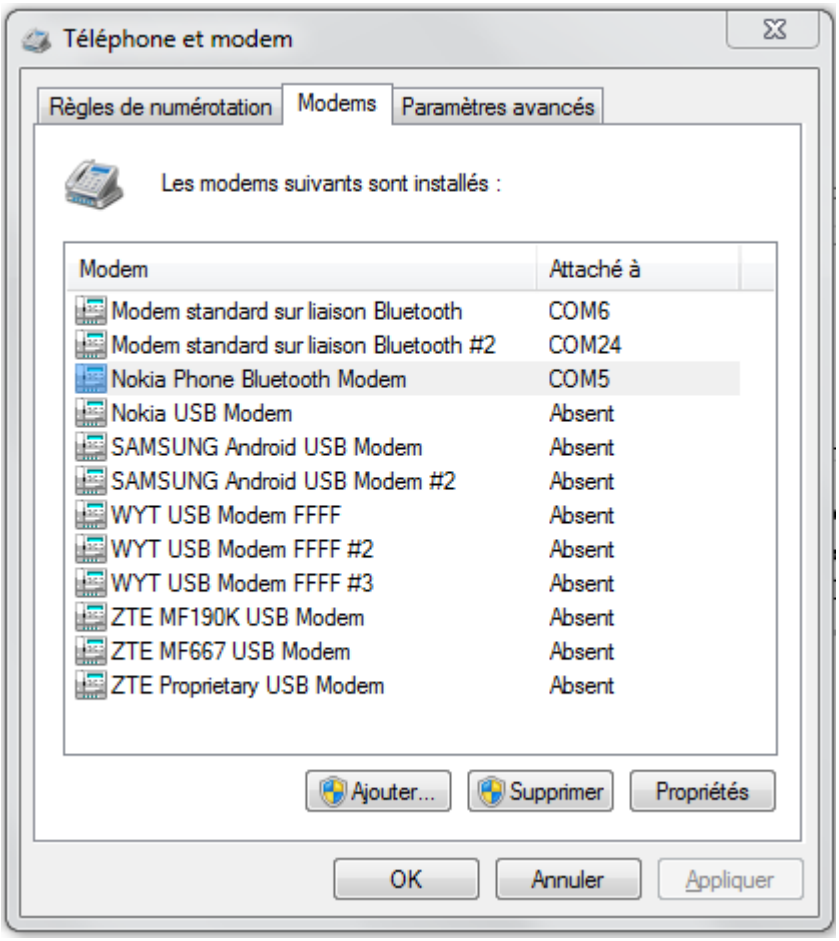

Figure 4.20: Récupération du port utilisé

Ensuite, la seconde étape consiste à configurer le téléphone jouant le rôle de caméra IP. Pour cela, on utilise l'application « IP Webcam ». Ainsi, ce téléphone et l'ordinateur hôte doivent être connectés sur le même réseau. Il ne reste plus qu'à récupérer l'adresse IP attribuée au téléphone. La figure 4.21 située à la page suivante schématise cette adresse IP.

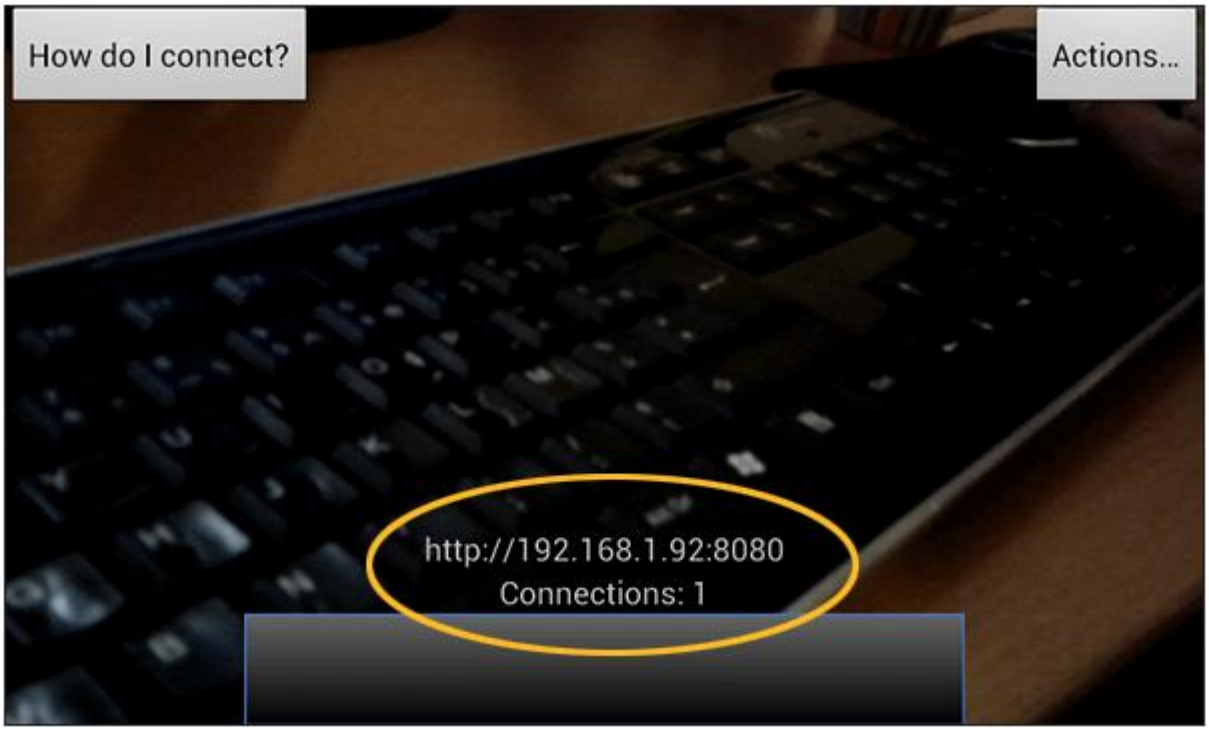

Figure 4.21: Récupération de l'adresse et du port

La dernière information utile est le numéro du téléphone à joindre en cas d'alerte.

Une fois toutes ces étapes effectuées, la sécurisation peut être activée.

En résumé, les informations fondamentales sont :

- l'adresse et le port de la caméra IP
- le port de communication avec le modem
- le numéro du téléphone à joindre

Il est à noter que, dans cet exemple, l'alarme SMS est activée et le niveau de sécurisation est réglé sur « Modéré ». Le répertoire d'enregistrement des images restant par défaut dans le document personnel.

Les configurations effectuées dans l'onglet « Général » et « Options Avancées » sont illustrées par les figures 4.22 et 4.23.

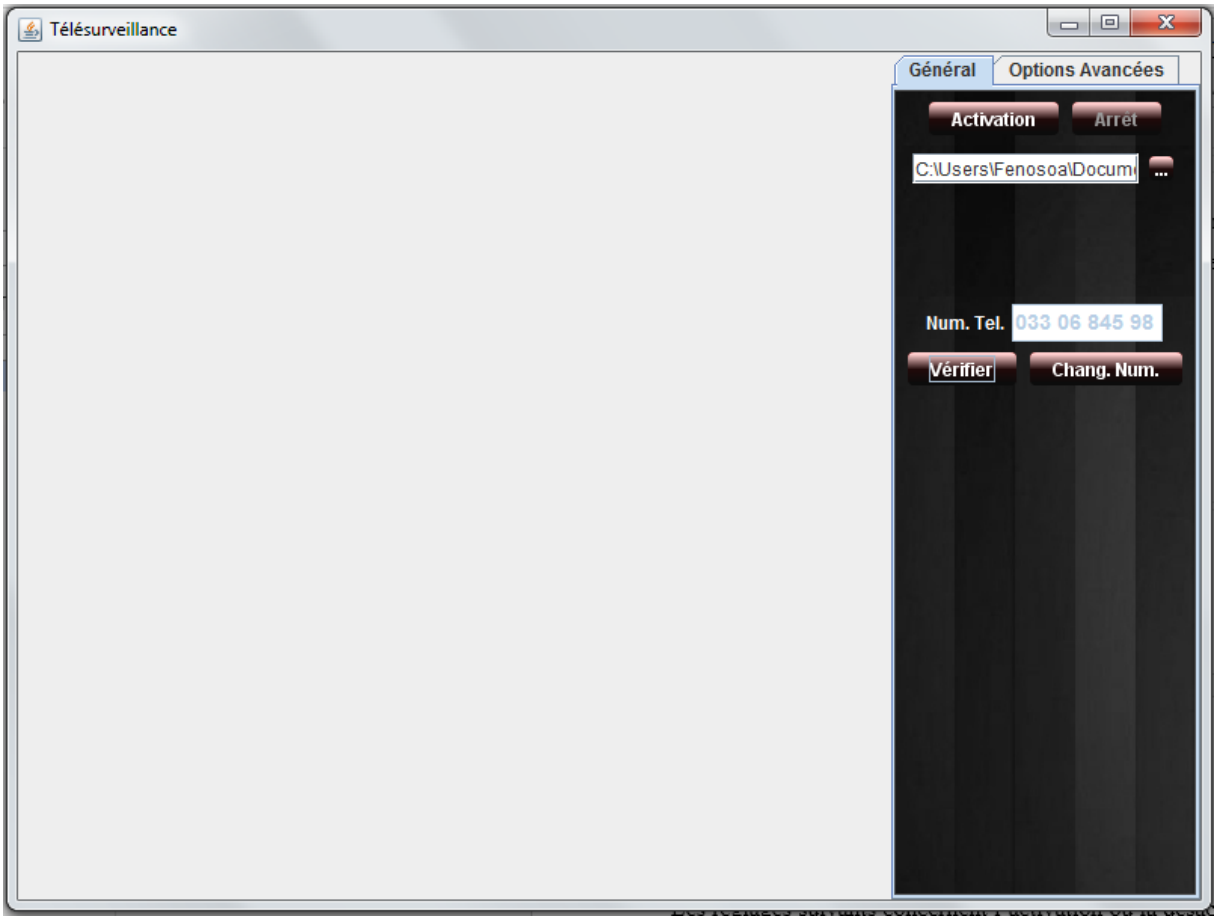

Figure 4.22: Interface "Général" configurée

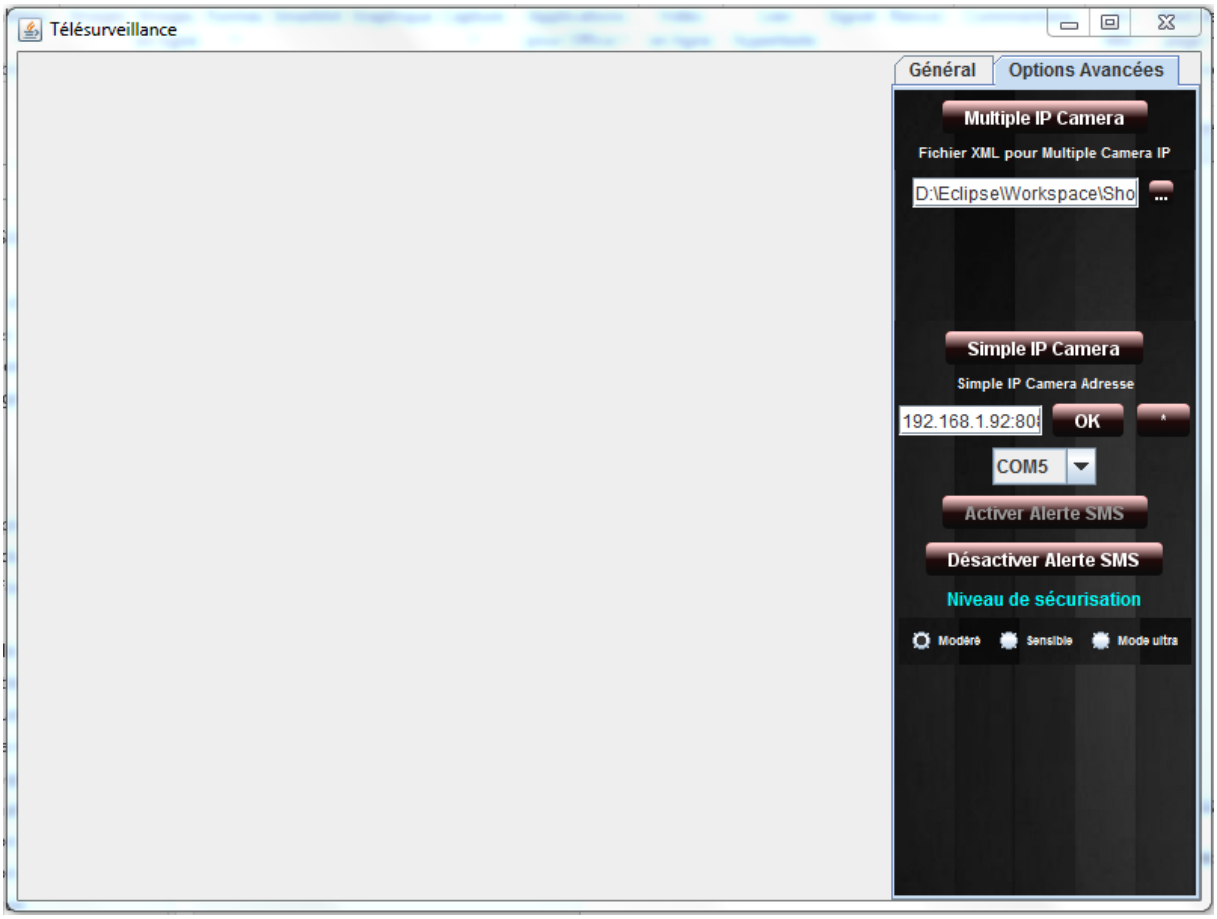

Figure 4.23: Interface "Options Avancées" configurée

4.5.2 Fonctionnement et résultats

Une fois le bouton « Activation » appuyé, l'application commence à sécuriser le site.

Cette sécurisation fait intervenir, en cas d'alerte, les différents matériels connectés. En effet, l'application réagit aux moindres mouvements suspects effectués dans le site. Dans ce cas, les images ayant provoquées l'alerte sont enregistrées dans le répertoire spécifié au cours de la configuration. Et suivant le degré d'imminence du danger, l'application déterminera si l'utilisateur doit être mis au courant ou non. Un exemple de message d'alerte envoyé à l'utilisateur et d'avertissement de danger imminent est illustré par la figure 4.24.

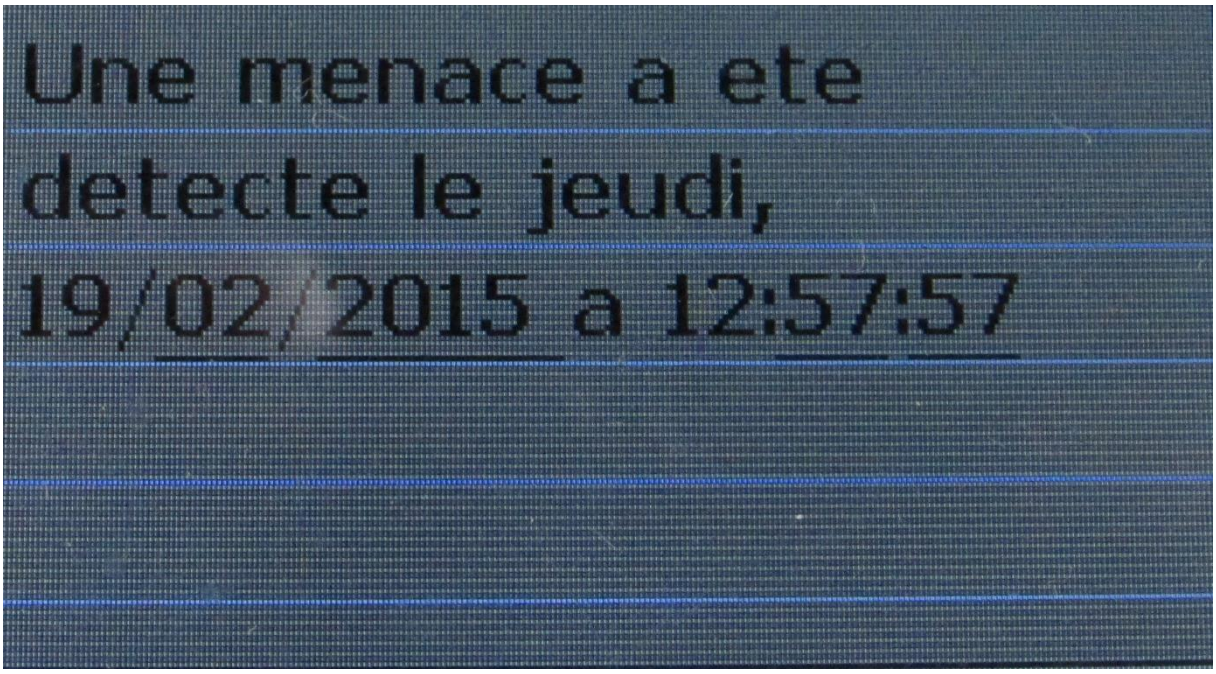

Figure 4.24 : Message d'avertissement

4.6 Estimation du coût de la réalisation

Désignations des tâches	Coûts estimatifs (Ar)
2 Smartphones	150 000 * 2
Main d'œuvre	150 000
Programme	300 000
Divers	15 000
TOTAL	765 000

Tableau 4.01: Estimation du coût de la réalisation

4.7 Conclusion

La notion de sécurisation nécessite une étude minutieuse des différents évènements qui peuvent se produire. A chacun des sujets étudiés correspond une solution adéquate. Ainsi, l'obtention d'un taux d'efficacité optimale requiert l'association de plusieurs techniques jouant chacune d'elle un rôle bien précis mais complémentaire. La dernière étape de la sécurisation dépend de la prise de décision effectuée par l'utilisateur.

CONCLUSION GENERALE

En guise de conclusion, cette application accroît considérablement le niveau de sécurisation d'un site. Mais ce niveau ne peut être atteint par n'importe lequel système de surveillance. L'efficacité d'un tel système réside surtout dans le fait de combiner différentes méthodes adéquates chacune à la résolution d'un type de problèmes. Dans le cadre de ce projet, l'application met en relief trois méthodes fondamentales assurant sa performance : la détection de mouvement servant à l'identification des malfaiteurs et des incidents survenus, le réseau GSM permettant d'informer l'utilisateur, et l'utilisation des caméras permettant la visualisation en temps réel des différents évènements. Toutes ces méthodes étant compatibles à la communication à distance, l'application assure la sécurisation du site même durant un voyage ou un déplacement effectué par l'utilisateur. L'application a été mise en place grâce au langage Java. Les principaux avantages de ce langage résident surtout dans le fait qu'il soit orienté objet et qu'il permette facilement de se déplacer d'un système informatique à un autre. Cette capacité à exécuter le même programme sur de nombreux systèmes d'exploitation différents représente un atout majeur pour cette application.

Cependant, malgré le haut niveau de sécurisation apporté par un système de télésurveillance, la dernière décision restera toujours au niveau de l'utilisateur. Le temps d'application des différentes solutions possibles suivant les problèmes encourus dépendra essentiellement des actions entreprises par l'utilisateur.

De nos jours, les logiciels et matériels de grandes marques ne cessent de subir des évolutions. Et cette application peut, elle aussi, faire le sujet de grandes améliorations telles que l'ajout d'une détection faciale et d'un système d'intelligence artificielle assurant la prise de décision en cas d'alerte imminent.

ANNEXE 1

EXTRAITS DE LA LISTE DE CAMERAS SUPPORTEES AVEC LES METHODES D'ACCES URL [17]

Marque	Modèle	Encodage de la vidéo	Accès URL
4xem	Generic snapshot	jpeg	/cgi-bin/video.jpg
Abus	TVIP21500	motion jpeg	/video.mjpg
ACTi	(generic mjpeg)	motion jpeg	/cgi-bin/cmd/system
Agasio	(generic mjpg)	motion jpeg	/videostream.cgi
Agasio	M105I	motion jpeg	/videostream.cgi
Apexis	(generic)	motion jpeg	/videostream.cgi
Apexis	APM-J011-WS-IRC	motion jpeg	/videostream.cgi
Apexis	APM-J012-WS	motion jpeg	/videostream.cgi
Aviosys	IP9100A	motion jpeg	/GetData.cgi
Axis	(generic)	motion jpeg	/axis-cgi/mjpg/video.cgi
Axis	2100	motion jpeg	/cgi-bin/mjpg/video.cgi
Axis	240Q	motion jpeg	/axis-cgi/mjpg/video.cgi
Axis	M1144-L	motion jpeg	/mjpg/video.mjpg
Axis	M1145-L	motion jpeg	/mjpg/video.mjpg
Axis	M7014	motion jpeg	/axis-cgi/mjpg/video.cgi
Axis	P7214 ch1	motion jpeg	/mjpg/1/video.mjpg
Axis	P7214 ch2	motion jpeg	/mjpg/2/video.mjpg
Axis	P7214 ch3	motion jpeg	/mjpg/3/video.mjpg
Axis	P7214 ch4	motion jpeg	/mjpg/4/video.mjpg
Generic		motion jpeg	/videofeed

Tableau A1.01 : Extrait de la liste de caméras supportées

ANNEXE 2

AJOUT DE LA FONCTION MODEM BLUETOOTH POUR NOKIA ASHA 306

Pour pouvoir utiliser un téléphone NOKIA en tant que modem, on doit se munir du logiciel NOKIA PC SUITE et suivre les étapes suivantes [18] :

A2.1 Installation de NOKIA PC SUITE :

- Se munir du programme d'installation de NOKIA PC SUITE disponible gratuitement sur le site officiel de Nokia
- Installez le logiciel
- Sélectionnez la langue, puis cliquez sur OK. L'assistant InstallShield Wizard lance alors le programme d'installation
- Lire et accepter le contrat de licence
- Dans la fenêtre « Sélectionner les applications », choisir d'installer toutes les applications
- Une fois l'installation terminée, redémarrez l'ordinateur

A2.2 Ajout du modem Bluetooth

- Activez le profil de connexion réseau à distance à partir de votre logiciel Bluetooth Windows. Activez Bluetooth sur votre téléphone, puis connectez votre téléphone à votre PC.
- Ouvrez le Panneau de configuration et sélectionnez « Téléphone et modem »
- Dans la boîte de dialogue « Téléphone et modem », sélectionnez l'onglet Modems. Dans la liste Modems, sélectionnez le modem Bluetooth que vous voulez mettre à jour. Cliquez sur Ajouter.
- Dans la boîte de dialogue Installer un nouveau modem, sélectionnez Ne pas détecter mon modem. Proposer le choix dans une liste. Cliquez sur Suivant.
- Dans la liste Fabricant, sélectionnez Nokia. Dans la liste Modèles, sélectionnez le modem que vous voulez mettre à jour. Cliquez sur Suivant.

- Sélectionnez l'option « Ports sélectionnés ». Dans la liste, sélectionnez le port COM sur lequel vous voulez installer le modem. Cliquez sur Suivant.
- Lisez la note dans la boîte de dialogue suivante. Cliquez sur Continuer pour continuer la mise à jour, ou sur Arrêter l'installation pour y mettre fin.

Le téléphone peut ainsi être utilisé en tant que modem Bluetooth.

ANNEXE 3

EXTRAITS DE CODES SOURCES JAVA

A3.1 Initialisation de la webcam utilisée et lancement de la détection de mouvement

```
Webcam webcam=Webcam.getDefault();

        BufferedImage imageDef,image,image1;
        WebcamMotionDetector detector=new WebcamMotionDetector(webcam);



            //définition de l'intervalle de temps pour la sensibilité
        detector.setInterval(niveau);
        detector.start();
```

A3.2 Gestion de l'envoi de SMS

```
//gestion date
SimpleDateFormat formater = null;
Date aujourdhui = new Date();
formater = new SimpleDateFormat("'le' EEEE, dd/MM/yyyy 'a' hh:mm:ss");
System.out.println(formater.format(aujourdhui));
message=message+formater.format(aujourdhui);
if(automatique){
        //initialisation du driver
        Win32Driver driver=new Win32Driver();
        driver.initialize();

        String[] tab = new String[100];
```

```
        //affichage et ajout des noms des ports dans le JComboBox
        while(portList.hasMoreElements()){

        portId=(CommPortIdentifier) portList.nextElement();
                                                        tab[z]=portId.getName().toString();

        System.out.println(portId.getName().toString());


        if(portId.getPortType()==CommPortIdentifier.PORT_SERIAL){
        memoire[a]=tab[z];
                                                                System.out.println("Memoire  =
"+memoire[a]);

        SerialConnection.port=portId.getName().toString();
        a++;

        }

        z++;


        }


        }
        //port préalablement choisi
        else{
                if(activationSMS){
                        try{
                                SerialConnection.port=nomPort;
```

```
                    sc.sendMessage(numero, message);
                }catch(NullPointerException e){
                    new JOptionPane().showMessageDialog(null, "Port série non valide","Message Informatif",JOptionPane.INFORMATION_MESSAGE);
                }
        }

}
```

BIBLIOGRAPHIE

[1] « *Télésurveillance* », *http://fr.wikipedia.org/wiki/Télésurveillance*, Octobre 2014.

[2] L. Beddiaf, « *VIDEOSURVEILLANCE, Principes et technologies* », 2008.

[3] J.F. Pillou, « *La lumière* », *http://www.commentcamarche.net/contents/1211-la-lumiere*, Juin 2014.

[4] F. Laissus, « *Réseaux locaux* », *http://www.laissus.fr/cours/node6.html*, Février 2009.

[5] « *Vidéosurveillance* », *http://fr.wikipedia.org/wiki/Vidéosurveillance*, Février 2015.

[6] « *Image numérique* », *http://fr.wikipedia.org/wiki/Image_numérique*, Novembre 2014.

[7] « *Caméra IP* », *http://fr.wikipedia.org/wiki/Caméra_IP*, Décembre 2014.

[8] « *Le modem* », *http://www.commentcamarche.net/contents/753-le-modem*, Février 2015.

[9] J.P. Muller, « *Bluetooth* », Janvier 2015.

[10] D.G. Frédéric, « *WiFi* », Novembre 2003.

[11] « *Wi-Fi* », *http://fr.wikipedia.org/wiki/Wi-Fi*, Février 2015.

[12] G. Marchal, « *QSP-revue* », Belgique, Novembre 2010.

[13] « *USB* », *http://www.commentcamarche.net/contents/773-usb*, Février 2015.

[14] J.P. Muller, « *Le réseau GSM et le mobile* », Juillet 2002.

[15] M.A. Rakotomalala, « *Radiocommunication mobile* », Cours L3-TCO, Dép. TCO.-E.S.P.A., A.U.: 2013-2014.

[16] « *Short Message Service* », *http://fr.wikipedia.org/wiki/Short_Message_Service*, Février 2015.

[17] « *Supported Cameras, NVRs & DVRs* », *https://www.mangocam.com/help/supported-cameras*, 2014

[18] « *Nokia PC Suite* », *http://nokia-pc-suite.helpmax.net*, Février 2014

FICHE DE RENSEIGNEMENTS

Nom : RATOVO

Prénom : Fenosoa

Adresse de l'auteur :

Lot II H 5 Faravohitra

ANTANANARIVO 101

MADAGASCAR

E-mail : ratovolightness@yahoo.fr

Téléphone : 033 06 682 55

Titre du mémoire :

« SECURISATION PAR TELESURVEILLANCE »

Nombre de pages : 75

Nombre de figures : 39

Nombre de tableaux : 6

Directeur de mémoire :

M. RAKOTOMALALA Mamy Alain, Maître de Conférences,

Adresse e-mail : rakotomamialain@yahoo.fr

Téléphone : 033 12 036 09

RESUME

La vie quotidienne de tout individu est souvent confrontée aux problèmes d'insécurité et de délit. La solution la plus efficace face à ces sujets se base essentiellement sur deux faits fondamentaux. La première concerne l'étude des différents cas pouvant se produire, la recherche d'une solution correspondant à chacun des cas, et la combinaison de toutes les solutions trouvées au sein d'une seule méthode formant la solution fondamentale. La seconde est la plus importante car elle se focalise surtout sur la prise de décision de l'utilisateur. Ce dernier représente l'élément clé de l'aboutissement d'un système de sécurisation. Partant de ce principe, l'application mise en place fait intervenir trois moyens permettant la résolution de différents problèmes, à citer : l'utilisation du réseau GSM, la possibilité d'évolution en fonction des avancées technologiques, et la résolution des problèmes en relation avec la distance.

Mots clés : Télésurveillance, Sécurisation, Webcam, Bluetooth, Wi-Fi

ABSTRACT

The daily life of every individual is often faced with insecurity and crime problems. The most effective solution addressing these issues is primarily based on two fundamental facts. The first one concerns the study of different cases that can occur, the search for a solution corresponding to each case, and the combination of all the solutions within a single method forming the fundamental solution. The second one is the most important because it focuses primarily on the decision of the user. This is the key to the outcome of a security system. On this basis, the application implementation involves three ways to solve different problems, including the use of the GSM network, the ability to change as technology advances, and solving problems related with distance.

Keywords: Remote Monitoring, Security, Webcam, Bluetooth, Wi-Fi