

La guerre du développement numérique

Menaces sur la confidentialité des photos numériques

Pierre DUSART¹ et Damien SAUVERON²

¹ LACO (UMR CNRS n°6090),
Faculté des Sciences et Techniques,
123, avenue Albert Thomas, 87060 Limoges, France

pierre.dusart@unilim.fr,
<http://www.unilim.fr/laco/>

² LMSI (EA2632),
Faculté des Sciences et Techniques,
83, rue d'Isle, 87000 Limoges, France
damien.sauveron@unilim.fr,
<http://msi.unilim.fr/>

Résumé De nos jours la photographie numérique tend à remplacer le développement argentique de part sa simplicité d'utilisation et du faible coût qu'elle engendre. Hélas, la facilité de copie qu'elle procure se transforme vite en désavantage pour le consommateur quand il s'agit de préserver la confidentialité de ses photos (c'est-à-dire sa vie privée). En effet, il est possible de faire des copies à l'insu et au détriment des utilisateurs. Afin de les tranquilliser, les laboratoires de développement photo mettent en œuvre des solutions telles que des CDs cryptés pour assurer la confidentialité des données lors des transmission entre l'utilisateur et le lieu de développement. Comme nous le montrerons, les méthodes de transfert actuellement utilisées ne sont pas suffisamment sûres. Nous illustrerons notre propos en montrant comment il est possible de lire les photos contenues sur les CDs cryptés. Cet article s'attachera à pointer les lacunes constatées et proposera quelques solutions. En résumé, aujourd'hui le développement numérique est beaucoup moins sûr que le développement argentique en terme de confidentialité.

1 Introduction

Aujourd'hui, le numérique se répand dans beaucoup de domaines mais surtout pour le grand public dans le domaine audio/vidéo. Après un engouement dans l'industrie musicale (CD, fichiers MP3, ...), le phénomène apparaît dans la vidéo (format DV) et dans la photo. Si le marché du développement des photos numériques n'a pas encore supplanté celui du développement argentique, il est en pleine expansion. En effet, les appareils photos numériques représentent par exemple déjà près du tiers des appareils photos existants aux États-Unis et les prévisions de croissance sont de 16 points de part de marché pour les 12 prochains mois [1]. Grâce à cette démocratisation de la photo numérique, tout un chacun peut créer, recopier et pratiquement produire son produit numérique sans intervention d'un professionnel. D'ailleurs, aujourd'hui seuls 5% des propriétaires

d'appareils numériques font développer leurs photos par un laboratoire. Inquiets pour leur avenir, les professionnels du développement photo (Kodak, Fujifilm, etc.) se livrent une guerre acharnée pour proposer de nouveaux services attractifs destinés à créer le besoin chez le consommateur. Ils entendent ainsi tenter de conserver leur clientèle, voire d'en capter une nouvelle. Parmi ces nouveaux services, les deux principaux sont la sauvegarde sur CD et le développement des photos numériques. En effet, un des défauts de la photo numérique est l'absence de tirage papier. Celui-ci peut être conservé dans un portefeuille, montré sans le secours d'appareils externes (ordinateur, lecteur DVD, etc.) et indépendant des formats spécifiques. L'autre défaut majeur provient du fait que tous les consommateurs ne disposent pas des moyens matériels (par exemple, un graveur) pour faire les sauvegardes de leurs photos sur CD.

Pour conserver leur emprise sur le marché et pour se rendre incontournables, la stratégie des laboratoires est double. Elle consiste à focaliser leurs nouveaux services numériques sur ces lacunes et à proposer des mini-services de proximité. Depuis quelques mois, de plus en plus de commerçants (photographes, bureaux de tabac, centres commerciaux, etc.) possèdent ainsi des bornes interactives en libre service qui permettent essentiellement deux choses à l'utilisateur : sauvegarder la mémoire de son appareil numérique (pour la vider ensuite) et commander des tirages de ses photos à divers formats. Si en soit ces nouveaux services n'ont rien de bien répréhensibles, ils posent tout de même de nombreuses questions éthiques et de sécurité (le respect de la vie privée – c'est-à-dire la confidentialité des données –, les droits de propriétés intellectuelles, etc.).

2 Le développement argentique classique

Les problématiques soulevées par le développement argentique concernent principalement le respect de la vie privée. Ainsi, le film « Photo Obsession » (*One Hour Photo*) [2] présenté au festival international du film de Sundance en janvier 2002 base son intrigue sur les menaces liées à la vie privée lors du développement de photos. Dans ce film, Sy Parrish (interprété par Robbin William) est un homme effacé et timide qui dirige depuis des années le laboratoire de développement rapide d'un supermarché. Depuis des années, les Yorkin sont une famille d'Américains modèles pour Sy, qui vit seul. Ils apportent leurs pellicules dans ce laboratoire. À défaut d'une famille, Sy ne peut s'empêcher de suivre leur évolution à travers les doubles de leurs photos.

Récemment, les médias ont montré un père, arrêté alors qu'il allait récupérer ses photos. Il était soupçonné de pédophilie suite à la dénonciation à la police d'un laboratoire de développement rapide. En effet, la pellicule photo qu'il avait fait développer contenait des photos d'enfants nus. Après enquête, on a découvert que sa petite fille avait pris en photo son frère nu mais également ses peluches avec un appareil jetable. Le père l'avait fait développer sans être à aucun moment au courant du contenu de la pellicule. Mais le mal était fait et le discrédit jeté sur cette personne.

Ces deux exemples sont donc des illustrations parfaites du principal problème éthique du développement argentique : le respect de la vie privée.

Dans le monde du développement argentique classique, il existe deux sortes de professionnels : les PhotoLab et les Laboratoires (Fujifilm, Kodak, etc.). Chacun possède des avantages mais aussi des inconvénients.

2.1 Les PhotoLabs : 1 h

Il s'agit de photographes qui ont investi dans un mini-laboratoire de développement rapide (1 heure environ). Les gros avantages des PhotoLab sont la proximité car il en existe plusieurs dans une même ville mais surtout la rapidité du développement. L'inconvénient majeur, qui est lié à la proximité, est la menace sur la vie privée. En effet, il y a de forte chance qu'une même famille fasse toujours développer ses photos dans le même PhotoLab. Le travail de l'opérateur consiste à faire les tirages puis à vérifier la qualité de développement de toutes les photos des clients. Ainsi, il a accès à une partie de leur vie, parfois intime (il connaît leur nom, leur vie au travers des photos, leur adresse, etc.). Si dans une grande ville, il y a peu de chance que l'opérateur ne (re)connaisse des clients ; il n'en est pas de même partout. L'opérateur peut donc simplement regarder les photos mais aussi en faire des copies dans des buts divers (collection personnelle, diffusion afin de nuire, diffusion dans un but commercial, etc.).

Par ailleurs, ces photographes proposent aussi souvent un service de développement en 24/48 h généralement moins cher que le développement rapide car associé à un laboratoire.

2.2 Les laboratoires de développement : 24/48 h

Ces laboratoires sont en fait des centres spécialisés dans le développement des pellicules pour plusieurs régions, voire un pays. Ils sont la propriété de grands groupes (Fujifilm, Kodak, etc.) spécialisés dans la vente de pellicules et d'appareils photographiques. Ils travaillent avec tous les photographes (même ceux qui proposent le développement 1 h), les comités d'entreprises, etc. Le fonctionnement global du système est assez simple :

- tous les soirs, un coursier passe chez les différents photographes affiliés pour récupérer les pellicules de tous les clients ;
- les pellicules sont transmises au laboratoire ;
- le laboratoire réalise les tirages et vérifie leur qualité ;
- les photos sont ensuite renvoyées par coursier aux photographes ;
- le client peut alors venir les récupérer 24/48 h plus tard.

Les avantages de ce système pour le client sont multiples. Il respecte plus sa vie privée puisque les opérateurs sont extérieurs à sa ville et qu'ils ne sont jamais en contact direct avec le client. De plus, comme le débit des pellicules traitées est plus important, il y a très peu de chance qu'un opérateur traite deux fois les tirages d'un même client. Ce fort débit dans le traitement des pellicules permet aussi au client d'obtenir un meilleur prix pour le développement de ses photos. De la même façon, le coursier ne peut pas facilement regarder et copier les photos

car cela exige beaucoup de temps. En revanche, le risque de perte ou de vol de la pellicule, des photos ou tout simplement leurs endommagements est plus important que dans le cas précédent à cause de la quantité des opérations requises (transport, etc.). Le problème du vol est très important et sera également abordé dans le cadre du développement numérique.

3 Le développement numérique

Si le numérique offre des avantages comme de pouvoir visualiser immédiatement les photos, de les détruire si elles sont ratées, de les dupliquer facilement, ce dernier aspect est à l'origine de la plupart des nouveaux problèmes que nous allons aborder.

Dans le cadre du développement numérique, les deux services à forte valeur ajoutée proposés par les laboratoires sont la création de CDs de sauvegarde et le développement des photos. Le consommateur a alors le choix entre différentes solutions techniques répondant à ses besoins :

- le laboratoire « maison » ;
- les bornes de développement numérique ;
- le développement numérique via l'Internet.

3.1 Le laboratoire « maison »

Il est possible de réaliser les deux services chez soi pour peu que l'on dispose d'un ordinateur équipé d'un graveur afin de réaliser le premier service et d'une imprimante de qualité photo pour réaliser le second service. Même si l'impression des photos est possible avec une imprimante spécifique photo, la qualité obtenue est bien inférieure à celles des travaux professionnels et d'un coût bien supérieur. En revanche, cette solution offre l'avantage non négligeable d'être totalement sécurisée en terme de confidentialité.

3.2 Les bornes de développement numérique

Pour les deux services, la première étape sur les bornes de développement numérique est toujours la même. Elle consiste à transférer les données numériques (la photo) du médium de départ (carte mémoire, téléphone portable, etc.) via une machine et un dispositif de lecture du médium source vers un médium temporaire (un disque dur).

Selon la nature du service demandé, la seconde étape consiste à transférer les données du médium temporaire :

- soit pour une sauvegarde, directement, vers un CD ;
- soit pour des tirages, vers les laboratoires de développement selon diverses méthodes de transmission des informations en fonction du commerçant choisi (impression directe, via un CD crypté, via une connexion Internet).

Généralement, le commerçant met à la disposition du client une borne multimédia libre service (cf. figures 1 et 2) qui permet essentiellement deux choses : lire le médium et faire une sauvegarde et/ou commander des tirages à divers formats de ces photos.



FIG. 1. Borne Fujifilm.



FIG. 2. Borne Kodak.

La sauvegarde sur CD

Le service de sauvegarde est payant avec des tarifs très divers (de 2,5 euros à 10 euros) sans justification apparente. Les bornes permettent ainsi au client de repartir avec un CD correspondant :

- à la copie d'une carte mémoire à divers formats ;
- à la copie de photos issues d'un téléphone portable intégrant un appareil photo et communiquant via IrDA ou BlueTooth ;
- à la copie d'un CD (sic!) ;
- à la copie de photos provenant de ces différents média.

En général, les CDs vierges n'étant pas en accès libre il faudra les demander au commerçant afin de les payer. Le problème qui se pose pour toutes ces bornes est celui de confidentialité puisque les photos passent par un médium intermédiaire (un disque dur) avant d'être gravées sur le CD. Par ailleurs des dispositifs pourraient être installés à l'intérieur de la machine pour récupérer les photos qui transitent.

En effet, le numérique offre une telle facilité de duplication et de stockage de l'information qu'il est possible de tout imaginer.

Le transfert des données vers le laboratoire

Au même titre que le service de sauvegarde, le service de développement est payant. Il permet au client d'obtenir ses photos sur papier au format choisi (le tirage coûte environ 0,5 euro par photo au format 6*8) mais également de recevoir une sauvegarde de ses photos sur CD (comme pour le service ci-dessus) à l'issue du passage par le laboratoire de développement. Selon le commerçant que choisit le client, il existe plusieurs types de borne réalisant ce service.

Le premier type de borne permet de faire un développement immédiat (dans les minutes qui suivent) des photos présentes sur le médium original. C'est, par exemple, le type de machine employé par la chaîne PhotoService. C'est sûrement pour le client les bornes les plus rassurantes en terme de respect de la vie privée car le développement se fait en direct et personne ne les manipule.

Le second type de borne est utilisé par les commerçants affiliés au laboratoire Kodak. Après avoir transmis ses photos (depuis le médium original vers la borne), après avoir sélectionné celles qu'il souhaitait développer et après avoir choisi le format de tirage ainsi que la multiplicité, ses photos sont transmises via Internet jusqu'au laboratoire pour développement. Puis, 24/48 h plus tard, le client récupère alors ses photos au magasin et éventuellement un CD de sauvegarde demandé après leurs retours par coursier. Dans ce cadre le problème de confidentialité se pose lors de la transmission des données du commerçant vers le laboratoire car il ne semble pas que le transfert soit sécurisé. Par ailleurs, même si ces communications étaient sécurisées, ces bornes étant connectées à l'Internet quelles garanties a le client que la machine n'a pas été piratée ?

Enfin le troisième type de borne est celui utilisé par les commerçants affiliés au laboratoire Fujifilm. À la suite du transfert des photos depuis le médium original vers la machine, de leur sélection, du choix du format et de la multiplicité, ces bornes gravent un CD crypté [5] contenant les photos si l'on en croit les affiches apposées à proximité. Une fois le CD gravé, il est placé dans une pochette sur laquelle doit être apposée une étiquette (éditée par la borne) détaillant la commande. Le CD est ensuite transmis par coursier au laboratoire Fujifilm et 24/48 h plus tard, le client récupère au magasin ses photos avec éventuellement un CD de sauvegarde si la demande a été formulée. Pour assurer la confidentialité des données du client, le contenu du CD transmis à Fujifilm n'est théoriquement déchiffrable que par le laboratoire. Ainsi, en cas de perte ou de vol, les données sont normalement inaccessibles. Mais est-ce réellement sûr ? Dans le cadre de cet article nous sommes allés développer des photos numériques sur une des bornes de Fujifilm, mais nous avons gardé le CD. Nous voulions développer les photos de « notre » CD nous-même afin de montrer que la confidentialité n'est pas assurée avec la cryptographie mise en place. D'ailleurs est-ce réellement de la cryptographie ? Pour parler en termes de cryptographie, il faut faire une cryptanalyse en dehors du cadre du principe de Kerckhoff puisque le principe de chiffrement n'est pas connu. Ici c'est une attaque à clair connu puisque l'on

connaît les photos que l'on a sauvegardées. La section 4 présente la procédure que l'on a mise en place pour retrouver nos images sur le CD. On a constaté qu'une fois la technique connue, nous pouvions également analyser le CD crypté de n'importe quel client et en découvrir le contenu. La méthode proposée est donc peu sûre en terme de confidentialité.

On notera que dans le cas des deux derniers types de borne la confidentialité des photos numériques ne peut pas être assurée lors du retour si un CD de sauvegarde a été commandé. Ce CD contenant les données lisibles par tout le monde, le vol du CD peut permettre leur récupération. Ainsi, aussi bien lors du transfert du CD crypté du commerçant vers le laboratoire (pour la solution Fujifilm) que pour le transfert du CD de sauvegarde du laboratoire vers le commerçant (pour les solutions Fujifilm et Kodak) un coursier malhonnête peut copier rapidement les photos à l'insu du client (s'il est capable de déchiffrer le CD crypté – par exemple avec la méthode que nous proposons).

Divers problèmes

Un problème commun aux différentes bornes permettant le transfert des photos via BlueTooth (par exemple depuis son téléphone portable) est une nouvelle fois la confidentialité. Une personne mal intentionnée pourrait essayer d'intercepter les données échangées. Certes, il faut être assez proche de la borne et sniffer une connexion BlueTooth est relativement difficile (cela requiert un matériel assez coûteux), mais ce n'est pas impossible.

Les problèmes liés à la possible capture de données pour les échanges IrDA sont eux très limités à cause de la faible portée de l'infrarouge et à sa convergence.

Un problème avec la borne libre service de Fujifilm est que les CDs destinés au laboratoire sont en libre service pour que les clients choisissent leurs photos et les gravent grâce à la borne en vue de les faire développer. Ainsi, il est possible de prendre une pile de CDs vierges pour graver ses données à la maison. Pour empêcher Monsieur tout le monde d'agir ainsi, Fujifilm laisse une session ouverte au début du CD afin de diminuer les risques de vols. Mais la fraude reste limitée car la borne est souvent proche du comptoir du commerçant où du personnel peut aider en cas de difficulté d'utilisation et également intervenir si la pile de CDs part d'un coup!

3.3 Le développement numérique via l'Internet

De nombreux sites web proposent les deux services que nous avons déjà décrits. Parmi eux, on trouve de grandes enseignes de supermarché (Cora, Carrefour, Géant, etc.) qui utilisent presque tous Kodak comme laboratoire de développement sous-traitant, mais aussi des chaînes de magasins de photo (Photo-Station, etc.) et des sites web totalement dédiés (PixDiscount, etc.).

Dans ce cadre, la première étape consiste à transférer des données du médium original vers une machine. S'il s'agit de la machine du client, il devrait pouvoir lui faire confiance. Bien évidemment dans les autres cas, la confidentialité des

photos pourrait être menacée. L'étape suivante est tout simplement le transfert des données de la machine vers le site du commerçant en ligne choisi. Lors de cette étape le client choisit les photos qu'il veut faire développer, le format, le nombre d'exemplaires, s'il désire un CD de sauvegarde ou pas. On constate que cette étape de transfert n'est pas sécurisée [3] et que donc la confidentialité de la vie privée du client ne peut pas être assurée. Enfin les résultats du développement papier (tirages) sont renvoyés :

- soit chez l'enseigne qui propose le service (par exemple un magasin Cora en France) auquel cas le client doit se déplacer pour récupérer ses tirages ;
- soit chez le client dans le cas de site web spécialisé ne possédant pas de comptoir physique.

Dans tous les cas le paiement se fait à la commande.

De la même façon que pour le cas des bornes, si le client a demandé une sauvegarde sur CD, lors du retour, le CD peut être intercepté et la confidentialité ne peut donc pas être garantie.

3.4 La charte d'utilisation

Avant d'utiliser ces bornes de développement ou les sites Internet, on peut lire la charte d'utilisation lorsqu'elle est présente. Il existe aussi de telles chartes pour le développement argentique mais les clients ne sont jamais informés de leur existence, sauf, peut-être, lors des cas de litiges [6,7]. Dans le cas du numérique, elles peuvent s'intéresser à des domaines qui s'étendent de la perte des données à la propriété intellectuelle en passant par le traitement que subiront les données. En revanche aucune n'aborde explicitement le problème de la confidentialité des informations lors de leur traitement ou alors de façon très parcellaire. L'utilisation des bornes étant possible même si la charte n'a pas été lue, en cas de problème l'utilisateur pourra certainement se retourner contre les laboratoires. Ainsi, sa lecture devrait être obligatoire. De plus, dans le cas des bornes de développement, un certain nombre de contraintes techniques afférentes aux bornes y sont décrites. Par exemple, on apprend dans la charte d'utilisation de Fujifilm que la transmission des données (du médium original) sur le support (sur le CD – c'est-à-dire la transmission interne à la machine) n'est pas protégée (ceci laisse sous-entendre que le reste l'est !). La présence de telles chartes est positive et pourrait être de nature à rassurer le consommateur si leur contenu ne rejetait pas toutes les responsabilités liées aux problèmes potentiels sur l'utilisateur.

Parmi les différentes chartes disponibles, celle de Fujifilm est la plus complète mais les points ci-dessous sont une compilation des réponses qu'apportent toutes ces chartes.

La perte

Afin de se protéger contre la perte des données, les laboratoires et les sites de développement solutionnent le problème en précisant qu'il est de la responsabilité du demandeur (c'est-à-dire du client) de s'assurer qu'il a fait une copie préalable pour la sauvegarde de ses données. Or, dans le cas d'une personne qui veut

sauvegarder sa carte mémoire sur un CD à l'aide d'une borne, il est évident qu'on est en présence d'un non-sens et même on pourrait dire d'un non-service (la borne offre le risque de perdre ses données au lieu de les sauvegarder!).

Le vol

Les chartes n'évoquent pas le cas de vol et considéreront le cas échéant un vol comme une perte puisqu'il est presque impossible de prouver un tel événement. Il est d'autant plus dommageable que cet aspect ne soit pas abordé que le numérique facilite le vol des données à l'insu de l'utilisateur, c'est-à-dire sans voler le support.

Les photos contrevenant aux lois

Les chartes d'utilisation préviennent que des images perçues comme contrevenant aux lois pourront être remises aux autorités chargées de faire respecter la loi. Par conséquent, cela signifie que les photos peuvent être examinées par des intervenants humains lors du développement.

L'effacement des données résiduelles

Peu de chartes précisent ce qu'il sera fait des données des clients à l'issue du développement. Celle de Fujifilm avertit le client que le CD crypté sera détruit au terme du processus de développement. À ce titre, le client doit donc avoir pensé à réaliser une sauvegarde de ses données. On notera le double coût pour le laboratoire, puisqu'un CD de transfert est détruit et qu'un nouveau CD de sauvegarde est gravé pour le client. Qu'advient-il des données transmises par Internet chez Kodak par exemple ?

La confidentialité ?

Les traitements des cas de perte de données, de vols et des photos contrevenant aux lois tels que décrit par les chartes laissent à penser que les laboratoires n'assurent donc pas la confidentialité des données transmises. L'argument de la confidentialité est pourtant souvent utilisé par les commerçants qui précisent que grâce au numérique les données sont traitées par des machines (et non plus par des humains) et qu'en conséquence le respect de la vie privée est plus important. Pourtant force est de constater que le numérique, utilisé comme aujourd'hui, restreint l'étendue de la vie privée.

La propriété intellectuelle

Concernant les droits de propriété intellectuelle sur les images à développer, les différentes chartes précisent qu'il est de la responsabilité du demandeur de posséder les droits de reproduction. En revanche, si les données du client étaient volées pour être utilisées commercialement, les chartes ne précisent en rien la responsabilité des laboratoires. Pourtant le préjudice pourrait être énorme si les photos sont de grande valeur (scoops, photos d'art, etc.).

3.5 La guerre économique

Pour capter les nouveaux clients de l'ère de la photo numérique, les laboratoires Fujifilm et Kodak se livrent à une guerre sans merci. Aujourd'hui, elle est stigmatisée par une guerre de prix (remise sur la facture lors de développement de lots de photos) mais également une guerre technologique (un CD versus l'Internet). Le but du CD crypté étant de rassurer le consommateur sur la fiabilité du transfert tant en terme de protection (pseudo-confidentialité) qu'en terme de matérialisation des données. Cette sécurisation du client se fait au dépend d'un délai de développement un peu plus long. À l'inverse, l'Internet fait peur car le consommateur le considère comme une zone de non-droit, donc peu fiable (pas de confidentialité), où les données sont dématérialisées (il n'y a pas de support) mais permet d'obtenir ses photos plus rapidement.

En parallèle, il y a également une guerre juridique. Par exemple, au départ, Fujifilm offrait le CD de sauvegarde à ses clients. Mais, sous la menace d'un procès intenté par un concurrent qui considérerait ce cadeau comme de la vente à perte (ce qui est illégal vis-à-vis des règles de concurrence), Fujifilm a décidé de faire payer le CD.

On pourrait également voir demain, des concurrents s'affronter technologiquement. Par exemple, un concurrent de Fujifilm pourrait très bien fabriquer un faux CD crypté – on va voir que l'on peut le faire sans problème à la section 4 – demandant l'impression des photos en 1 milliard d'exemplaires (et apposer sur la pochette du CD une étiquette qui n'est pas en conformité avec la « commande »). Si le système de duplication de Fujifilm est totalement automatisé, cela permettrait au concurrent de lui faire perdre beaucoup d'argent.

4 La récupération des photos sur le CD crypté

Dans cette section, nous présentons la méthode permettant de retrouver les photos sur le CD crypté de Fujifilm. Elle se décompose en trois étapes :

- la récupération de la session cachée contenant les images ;
- l'extraction de fichiers images corrompues ;
- le retrait des données factices introduites dans le format image.

4.1 La récupération de la session cachée

Pour récupérer la session contenant les données intéressantes d'un CD crypté de Fujifilm, il suffit de l'insérer dans un graveur de CD. En effet, sur un lecteur de CD classique, seule la première session qui est fermée, est lisible. Or, c'est dans la deuxième session, non fermée (et donc illisible par un lecteur classique) que se trouvent les images. Il s'agit ici de la première protection mise en place par le laboratoire Fujifilm. Nous avons choisi d'utiliser le logiciel *Easy CD Creator* pour extraire la session 2 et créer son image au format de fichier ISO. Ce fichier contient toutes les informations nécessaires pour décoder les images.

4.2 L'extraction des fichiers images corrompus

L'analyse de ce fichier ISO nous a conduit à constater que la session 2 contient les images à la suite séparées par des parties inintéressantes. C'est là, la deuxième protection du CD. Ainsi, pour retrouver les images (au format JPEG), il suffit de repérer dans le fichier ISO les entêtes des fichiers JPEG qui serviront de marqueurs de début ([4]). Une fois, leurs signatures trouvées, il suffit de chercher la fin des images pour obtenir des fichiers images. Lors de notre test, nous avons constaté que les tailles des images obtenues étaient plus importantes que celles des images originales.

4.3 La reconstruction des images

Une analyse des fichiers images a fait apparaître qu'elles contenaient des bouts de fichiers rajoutés. C'est la troisième protection. Ces morceaux de fichiers sont de longueur fixe (11Ch octets) et se répètent de façon périodique (tous les 800h octets lus soit aux positions 800h, 1000h, 1800h, 2000h, 2800h, ... de chaque image). Une fois ces morceaux de fichiers inutiles retirés, les images obtenues sont alors identiques aux images initiales. Les fichiers sont donc complètement lisibles par n'importe quel logiciel ouvrant le format JPEG.

4.4 Les inconvénients constatés

Ce mode de chiffrement augmente la taille du contenu du CD sans augmenter la quantité d'information. Les informations nécessaires sont les images et les informations client (nom, adresse et quelles images le client souhaite faire tirer, leurs formats et le nombre d'exemplaires).

4.5 Intérêts de casser ce médium

Les intérêts sont multiples pour une personne qui souhaite sauvegarder et retrouver ses photos de vacances alors qu'elle est en déplacement sans possibilité de décharger sa carte mémoire vers un ordinateur ou un disque dur indépendant. À ce moment là, la personne va chez un commerçant disposant d'une borne Fujifilm en libre service, elle vide sa carte mémoire sur le CD et repart avec le CD puisque rien ne l'oblige à faire développer le CD immédiatement. Le CD étant crypté, elle pourrait le faire développer dans un autre magasin proposant les bornes Fujifilm (par exemple, à son retour de vacances). Le cryptage du CD est aussi censé empêcher de faire développer le CD par un laboratoire concurrent.

Casser le cryptage du CD peut également permettre à un concurrent de mettre en place une guerre technologique ou à une personne mal-intentionnée dans la chaîne de développement de copier les images des clients pour en faire un usage frauduleux.

4.6 Commentaires de Fujifilm

Selon Fujifilm le CD n'est pas crypté pour assurer la confidentialité. Ce procédé et l'affichage préventif du magasin sont uniquement mis en place pour éviter le vol des CDs en libre service. D'ailleurs ils n'entendent pas modifier le système et la distribution des CDs sera contrôlée par le commerçant en cas d'abus.

5 Propositions de solution

Dans le cadre du transfert des photos via Internet (pour la borne Kodak, ou pour les sites de développement en ligne) nous proposons d'utiliser SSL (Secure Socket Layer) car même si ce mécanisme requiert plus de ressources et rallonge la durée du transfert, c'est la seule façon d'assurer un peu de confidentialité.

Dans le cadre du CD crypté de Fujifilm, nous proposons d'utiliser des vrais mécanismes cryptographiques pour assurer la confidentialité des données et ne pas perdre de la place inutilement sur le CD. Concernant le vol des piles de CDs sur leurs bornes, Fujifilm pourrait également intégrer dans ses bornes un automate qui mettrait lui-même les CDs dans le graveur.

De plus, dans les deux cas la borne est en réalité un PC et dispose donc de ressources de calcul suffisantes pour assurer un vrai chiffrement en temps réel des données.

Par ailleurs pourquoi ne pas adapter le contenu au tirage à faire (pourquoi sauver une image 6 Méga-pixels pour un tirage 10*15?)? Pourquoi ne pas développer l'interopérabilité, c'est-à-dire pouvoir permettre de sauver ses photos chez un marchand puis prospecter ailleurs pour les tirages (par exemple, là où c'est moins cher)?

6 Conclusion

Nous avons pu montrer qu'il existe des problèmes sur le CD Fujifilm mais il est vraisemblable que les autres solutions ont aussi leurs faiblesses. Comme nous n'avons pas eu librement accès à la manipulation des bornes Kodak, nous n'avons pas pu expérimenté des attaques. En substance, nous avons vu qu'il existait des problèmes de confidentialité pour le développement argentique que le support numérique amplifie. Les solutions actuellement mises en œuvre sont très faibles et reposent exclusivement sur l'ignorance du consommateur. Ainsi, on peut donc considérer aujourd'hui le développement numérique comme beaucoup moins sûr que le développement argentique en terme de confidentialité. Nous pensons que cela est dû à une croissance trop rapide du marché du numérique mais que demain des solutions plus performantes seront disponibles afin de garantir au consommateur le respect de sa vie privée tout en lui offrant les avantages de la photo numérique.

Références

1. FUJIFILM.
The Right Solution Not Just Any Solution.
<http://www.fujifilm.com/JSP/fuji/epartners/bin/AladdinBrochure.pdf>
2. Mark ROMANEK.
Photo Obsession (VF).
http://www.allocine.fr/film/fichefilm_gen_cfilm=28728.html
One Hour Photo (VO).
<http://www.foxsearchlight.com/onehourphoto/index.shtml>
3. PhotoStation.
Le verrouillage SSL (Secure Socket Layer) est-il utilisé ?
<http://www.photostation.fr/informations/faq.php>
4. Petit didacticiel sur les entêtes JPEG.
<http://www.vbfrance.com/code.aspx?ID=8575>
5. Absolut Photo.
Comment utilisez-vous le numérique ?
<http://forum.absolut-photo.com/ftopic3342-15.php>
6. Pascal KOBER.
Perte d'une pellicule par un laboratoire.
<http://perso.wanadoo.fr/pascal.kober/07livre/21laboratoire.htm>
7. Voyage Forum.
Cas de perte d'une pellicule par des laboratoire et jurisprudence.
http://voyageforum.com/voyage/negatifs_perdus_par_kodak_D122577/