L'analyse numérique d'images au service de la protection des documents imprimés

par Roland Meylan
AlpVision SA

Résumé

Les moyens informatiques matériels, tels que les photocopieurs couleur, les scanners et les imprimantes, de même que les logiciels de retouches d'images de plus en plus sophistiqués, disponibles à très peu de frais dans la grande distribution, permettent aux fraudeurs de tous bords de produire des falsifications de documents de plus en plus sophistiquées.

Cependant, ces mêmes moyens aux mains des responsables de la sécurité des entreprises et des organisations, peuvent également générer des protections efficaces, détecter les documents frauduleux et lutter efficacement contre les fraudeurs, aussi bien internes qu'externes à l'entreprise.

Ces nouvelles technologies de protection numérique sont de plus très faciles à déployer dans le cadre des systèmes bureautiques intégrés de toutes tailles et de toutes natures.

Allons-nous vraiment vers une société sans papier?

Sur la base d'une étude menée aux USA en 2003 par l'Université de Californie[1] et sa "Berkeley School of Information", le nombre de documents imprimés dans les bureaux des entreprises a augmenté de 43% entre 1999 et 2002.

Le nombre de pages imprimées par les employés des entreprises continue d'augmenter[2]. Il est donc évident qu'il n'y a pas de tendance nette de réduction de la consommation de papier à cause de l'usage de plus en plus massif des ordinateurs de bureau connectés.

Bien au contraire, il y aurait plutôt une relation entre l'augmentation des pages imprimées et l'augmentation de l'usage de l'ordinateur à l'échelle individuelle. Cela semble particulièrement vrai pour les contrats, les permis, les certificats et autorisations de toutes natures. Ces types de documents imprimés prolifèrent dans le monde entier.

Les fuites de documents confidentiels, les falsifications et contrefaçons se multiplient et ceci dans les entreprises et les organisations de toutes sortes, la plupart du temps par le fait d'employés indélicats. Cela s'explique peut-être par le développement constant des équipements d'impression et de scanner numériques ainsi que des logiciels de retouches d'images de haute performance, maintenant du ressort de l'informatique personnelle de grande diffusion, donc accessibles à chacun.

Quels sont les enjeux de la protection des documents imprimés?

Une récente étude publiée par Price Waterhouse Cooper en 2005[3] mentionne que 45% des entreprises dans le monde et 47% des entreprises françaises ont été victimes d'actes de criminalité économiques au cours des années 2003 et 2004. Les causes identifiées sont en

particulier la rupture de confidentialité, la falsification et la contrefaçon de documents légaux et financiers. Plus la compagnie est grande, plus elle est exposée à la fraude. Cela s'explique par le fait que les employés des grandes sociétés se sentent plus anonymes comparés à ceux des plus petites entreprises.

Les actes criminels touchant aux documents imprimés peuvent donc prendre plusieurs formes, comme par exemple :

- la diffusion de documents confidentiels;
- la falsification de documents par la modification d'éléments contenus dans le document original;
- la création frauduleuse de documents, soit la contrefaçon de documents.

Comment protéger efficacement les documents imprimés de valeur ou confidentiels?

Dans un environnement d'entreprise, on a vu plus haut que la criminalité interne est importante dans les grandes entreprises. Il y a lieu de se protéger aussi bien des infractions internes que des tentatives de tiers externes à l'entreprise. Plusieurs aspects doivent donc être considérés:

- une sécurisation visible ou invisible;
- une solution résistante à la photocopie et à la transmission par facsimilé;
- une résistance à l'élimination ou à l'altération de l'élément de sécurité;
- la distinction entre un original et une photocopie;
- une détection sur un fragment de document;
- une pérennité de l'élément de sécurité en cas d'archivage prolongé;
- une intégration aisée dans le flux existant du système bureautique de l'entreprise;
- une capacité à traiter la détection de l'élément de sécurité de manière automatique et industrielle, en cas de production massive;
- etc.

Ces quelques considérations montrent qu'il n'y a pas de solution universelle et unique pour la protection de documents imprimés. Vu les progrès constant des équipements potentiellement aux mains des fraudeurs, il est nécessaire que les fournisseurs de solutions continent à développer des parades. Une combinaison de diverses techniques est souvent une solution qui permet de répondre à des demandes de protection variées pour un même document. C'est par exemple une technique largement adoptée pour les billets de banques, qui contiennent plusieurs techniques de protection.

Quelles sont les diverses techniques de protection à disposition?

Une possibilité de classer ces techniques est de les séparer en procédés visible et invisibles.

Une protection visible est assez facilement identifiable et dans un sens «labellise» le document comme sécurisé. Cependant, par définition, une solution visible l'est aussi des fraudeurs, qui peuvent développer une contrefaçon à vue, jusqu'à ce que celle-ci paraisse acceptable comparée à l'original.

Une solution invisible est bien plus difficilement identifiable, sauf indiscrétion de la part des employés ayant contribué à sa mise en œuvre. On voit alors qu'une procédure de sécurisation est une chaîne d'éléments pour lesquels confidentialité et discrétion sont de rigueur. Ceci explique aussi pourquoi très peu de publications sont faites par les entreprises qui ont mis en place des procédés de sécurisation documentaire.

Des techniques visibles bien connues sont par exemple les codes à barre en deux dimensions, les impressions de microstructures ou l'adjonction d'éléments additionnels tels que des hologrammes ou des kinégrammes. L'information contenue dans ces éléments graphiques peut aussi être chiffrée.

Leur visibilité reste cependant une de leur faiblesse évidente, car elle permet leur éradication aisée par exemple.

Les techniques de protection invisibles explosent véritablement dû notamment au développement de machines d'impression de très haute qualité. Un récent article paru dans le *Washington Post* (Oct. 2005) [4] mentionne que plusieurs fabriquants d'imprimantes pour le bureau à domicile ou l'entreprise les ont livrées avec un procédé imprimant des marques invisibles sur chaque page, ceci à l'insu de leur utilisateur. Le but de ce procédé est de pouvoir identifier l'imprimante en cas d'usage frauduleux. Mise à part l'implication politique et légale d'un tel procédé, il démontre au moins que l'impression d'information invisible est possible aujourd'hui avec de l'encre normale et des imprimantes standard vendues dans le commerce.

La figure suivante illustre comment des points imprimés deviennent invisible à l'œil nu en fonction de leur taille et de leur couleur.

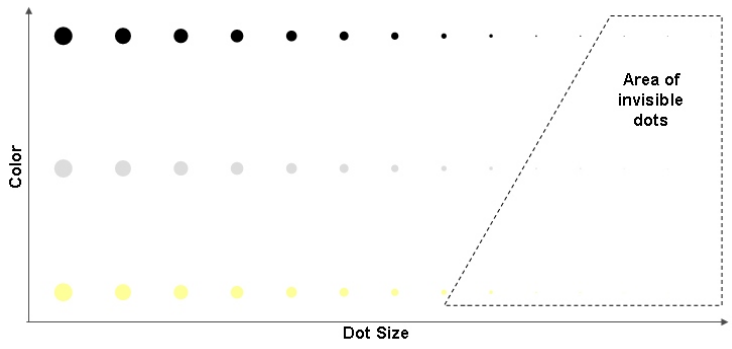


Fig. 1: Zone d'invisibilité à l'œil nu pour des points imprimés en fonction de leur taille et de leur couleur.

D'autres formes invisibles à l'œil nu de protection peuvent altérer légèrement la forme des lettres afin d'y encoder une information. Dans le jargon des technologies de sécurité, on les regroupe dans la catégorie des filigranes de textes ou «Text Watermarking» en anglais.

Là encore, la nature du document et de la protection à considérer va conduire à une solution appropriée ou à une combinaison de solutions.

D'autres solutions invisibles peuvent exiger l'apport d'éléments additionnels, tels que des encres spéciales réagissant à la chaleur ou à des longueurs d'ondes lumineuses bien précises, voire à des marqueurs chimiques apparentés à des codes DNA.

La figure ci-dessous classe ces différentes solutions en fonction de leur rapport efficacité/prix. Il prend en compte non seulement le coût d'un éventuel élément additionnel de sécurité, mais également le coût de l'implémentation dans la chaîne de traitement documentaire, ainsi que le coût de la détection de l'élément de sécurité pour la validation.

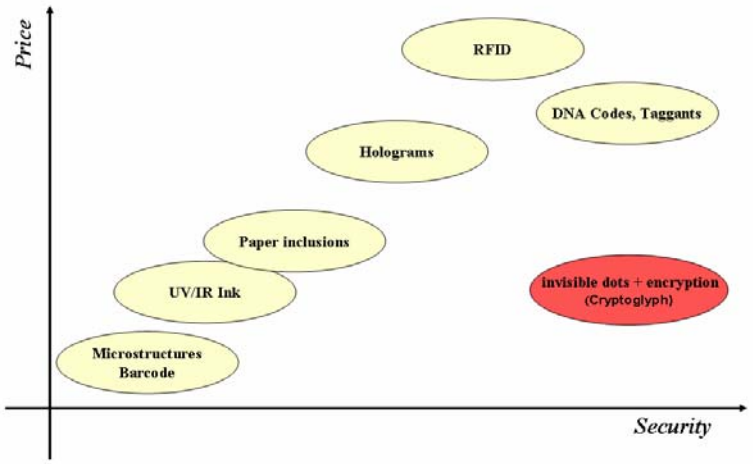


Fig. 2: Différentes techniques de protection visibles et invisibles

La détection des éléments de sécurité cachés dans les documents

Une autre question importante à laquelle doit répondre une spécification de sécurisation documentaire est la capacité de traiter les documents de manière industrielle. Les banques et les grandes compagnies, les administrations gouvernementales traitent des millions de documents. Il est alors impératif que le système choisi soit automatisable non seulement du point de vue de la détection des documents frauduleux, mais aussi que le procédé de génération des éléments de protection soit parfaitement intégré au système en place pour la production des documents informatisés imprimés.

Actuellement le chiffrement d'information par le biais d'éléments imprimés invisible représente la solution la plus efficace, pour autant que le chiffrement soit suffisamment solide pour résister à toute attaque. Le filigrane de texte semble aussi très prometteur, chacune des solutions a aussi des caractéristiques bien précises quant à sa capacité à résister ou non à la photocopie et à la transmission facsimilé.

Une solution d'impression numérique à été récemment commercialisée qui combine deux éléments[6]:

1. L’impression invisible à l’œil nu de micro-points sur une partie ou sur la totalité du document. Si la zone de présence de ces points est suffisamment grande, il est alors impossible de répliquer ces points ou de les éradiquer.

2. Ces micro points invisibles contiennent une information chiffrée par une clé de 128 bit, soit aussi puissante que celles utilisées dans les transactions bancaires. Si la détection est exécutée dans un endroit sûr, la clé n’est jamais exposée et le déchiffrement de l’information par des fraudeurs est impossible.

L’image ci-dessous montre combien il est difficile de distinguer une surface couverte de points imprimés d’une surface qui ne l’est pas. La raison en est simple: les imperfections naturelles du papier ou les traces laissées par l’impression laser par exemple confondent l’observateur, même sous agrandissement.

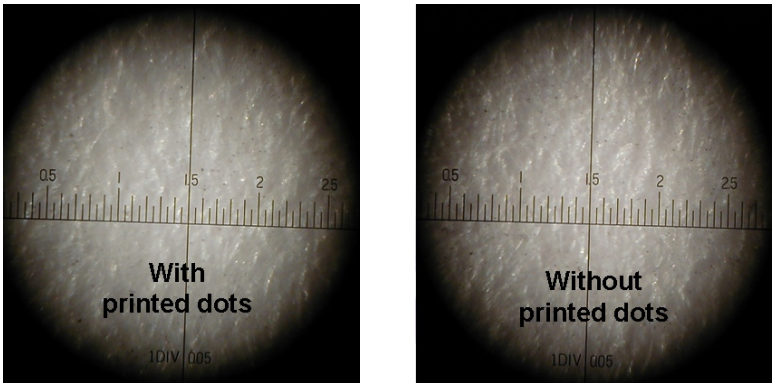


Fig. 3: Agrandissement d’une zone imprimée avec et sans points de marquage (1200 dpi noir/blanc)
Imprimante Laser sur papier blanc (une division = 0.05 mm)

Cette technique de camouflage qui utilise les imperfections du support imprimé permet donc de protéger une page blanche, comme une page imprimée. C’est un des aspects uniques et brevetés de cette technologie. La détection des points de marquage est basée sur des techniques avancées de signaux à très faible rapport signal sur bruit, qui permet en quelque sorte de retrouver une petite aiguille dans une immense botte de foin.

Ces micro-points sont intégrés au document juste avant l’impression, d’une manière parfaitement transparente pour le logiciel de traitement de texte utilisé pour créer le document à imprimer.

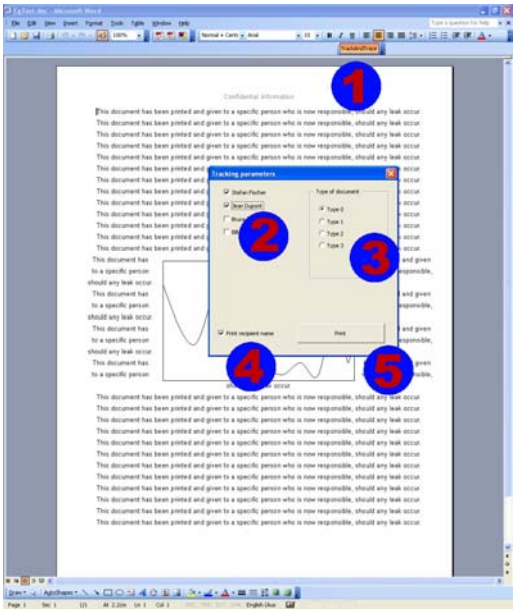
L’information cachée et chiffrée contient généralement une copie d’une ou plusieurs informations importantes imprimée sur le document (montants, date, origine, etc.). Si un fraudeur tente de modifier ces éléments visibles, la comparaison lors de la détection de ces éléments modifiés et de ceux chiffrés dans la protection invisible révélera immédiatement la fraude.

Si la protection doit résister à la photocopie, les micro-points seront rendus plus visibles, et la protection sera fournie par la clé de chiffrement qui permettra d’authentifier une photocopie valable.

Si on veut pouvoir distinguer l'original unique, on rendra les points invisibles et ceux-ci ne seront pas reproduits de manière fiable sur la copie, ce qui permettra de distinguer l'original de la copie.

L'autre élément intéressant est la très haute redondance de l'information cachée dans les marques de sécurité. Cela permet de retrouver cette information sur une portion de document, au cas où ce dernier aurait été déchiré, et ceci même plusieurs années après son impression. C'est donc un moyen d'identifier des fuites pour autant qu'on ait caché le nom ou le code de l'auteur et du destinataire d'un document confidentiel.

Un exemple d'interface de protection documentaire contre les fuites internes intégré à MS Word, qui permet avec quelques clics de générer un document imprimé aussi unique qu'une empreinte digitale.



1. On décide si on veut appliquer la procédure de sécurisation en cliquant sur une icône intégrée à la barre des menus.
2. On sélectionne la liste de distribution.
3. On sélectionne le type de document.
4. On décide si le nom du destinataire sera imprimé ou non en clair.
5. On imprime le document protégé.

Fig. 4 : Exemple d'intégration d'une protection contre les fuites internes dans MS Word.

La détection de l'information cachée et chiffrée se fait par un simple scanner à plat ou par un scanner industriel pour du traitement massif, piloté par le logiciel spécifique de détection.

Conclusions

Il n'y a pas de solution unique et universelle de sécurisation de documents imprimés. Une combinaison de solutions visibles et invisibles est souvent indispensable pour décourager soit les fraudeurs «à la petite semaine», soit les organisations criminelles aussi bien équipées que les producteurs des documents originaux.

Chaque solution devra donc être adaptée aux besoins spécifiques. De même, le niveau de protection souhaité devra être mesuré en fonction de son coût.

Le coût total d'une solution de sécurisation de documents imprimés doit englober l'ensemble des éléments : la création de la sécurisation, la détection et le management de l'ensemble.

Enfin, la solution doit être compatible avec un traitement automatique industriel en cas de production massive de documents.

L'auteur

Roland Meylan est ingénieur diplômé de l'Ecole Polytechnique Fédérale de Lausanne et au bénéfice d'une formation en administration d'entreprises de l'IMD Lausanne. Il est directeur de la communication de la société AlpVision SA à Vevey en Suisse, leader dans le développement de solutions numériques pour la lutte contre les contrefaçons aussi bien des produits que des documents.

La société a obtenu en 2004 le «Sceau Européen d'Excellence» pour ses solutions numériques de protection de documents imprimés. AlpVision a notamment collaboré avec la Société Générale de Surveillance – SGS à Genève pour la mise au point d'un système de protection documentaire pour le gouvernement éthiopien. La société a également développé, en collaboration avec des banques, un système de protection des ordres de paiement. Des millions de documents et de produits sont aujourd'hui protégés par les solutions numériques d'AlpVision.

AlpVision SA, rue du Clos 12, CH-1800 Vevey, tél. +4121 948 6464
www.alpvision.com info@alpvision.com

Références

[1] How much information 2003? http://www.sims.berkeley.edu:8000/research/projects/how-much-info-2003/

[2] A Society Addicted to Paper – The Effect of Computer Use on Paper Consumption, Geoffrey Peters, School of Computing Science, Simon Fraser University, Vancouver, B.C., Canada V5A 1S6, gpeters at sfu dot ca, March 12, 2003.
http://www.sfu.ca/~gpeters/essays/paper.htm

[3] Enquête sur la fraude dans les entreprises en France, en Europe et dans le monde, 2005, Dominique Perrier associée responsable du département Litiges & investigations, Price Waterhouse Coopers en France.
http://www.pwcglobal.com/gx/eng/cfr/gecs/PwC_GECS05_France.pdf

[4] Online Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg

[5] Document security program for Ethiopian government,
http://www.pstm.net/article/index.php?articleid=793

[6] Covert security technology, http://www.alpvision.com/cgoverview.html