L'INTERDICTION DE CACHETER SON COURRIER ÉLECTRONIQUE

Certaines expériences faites récemment sur la stéganographie en utilisant des images ne laissent aucun doute sur la possibilité de transmettre secrètement et rapidement de grandes quantités d'informations sur le réseau *Internet*.

La méthode de transmission par les images numériques est facile à mettre en œuvre, en voici le principe. L'émetteur du message secret envoie une image à son correspondant, dans laquelle il a modifié quelques pixels dont l'emplacement a été convenu ; ces pixels ont été remplacés par d'autres dont les numéros codent les lettres du message *(voir la figure 5)*. Si le nombre de pixels modifiés est assez faible, il est impossible de détecter quoi que ce soit en regardant l'image très peu modifiée qui circule sur le réseau. Le décodage est extrêmement facile : pour l'effectuer, il suffit de collecter les numéros codés dans les pixels aux emplacements convenus, de les interpréter pour reconstituer le texte secret que personne n'aura repéré dans l'image transmise. Des logiciels utilisant des versions perfectionnées de ce principe (et, pour certains, prenant en compte les difficultés introduites par les algorithmes de compression qui ne restituent pas parfaitement les images) peuvent être trouvés en passant par l'adresse *Internet* :

http://adams.patriot.net/~johnson/html/neil/stegdoc/stegdoc.html

Si l'on veut aujourd'hui surveiller tout ce qui transite par les réseaux informatiques, il ne suffit donc pas d'interdire par un règlement quelconque de coder les messages qui y circulent et d'aller ennuyer ceux qui ne respectent pas la loi, il faut aussi repérer tous les messages dissimulés par des méthodes de stéganographie, ce qui semble impossible. Pour rendre plus difficile encore la détection des messages cachés, les spécialistes recommandent de coder les messages que l'on noie. À la place d'images, on peut utiliser des sons ou des textes de programmes dans lesquels, par exemple, on redoublera certains blancs (ce qui est sans effet sur le fonctionnement du programme) pour marquer des emplacements spéciaux.

La loi française, une des plus répressives au monde en matière de cryptographie, est donc absurde et inutile malgré les modifications adoptées en juin dernier par les parlementaires. Elle restreint l'usage des méthodes cryptographiques, obligeant ceux qui veulent s'en servir à déclarer les méthodes qu'ils utilisent et à communiquer les clefs de codage à des «tiers de confiance». À l'heure actuelle, les décrets d'application ne sont pas parus, mais il est probable que les tiers de confiance à qui on devra confier les clefs seront aussi les vendeurs exclusifs des moyens de cryptographie autorisés et qu'en conséquence le cryptage sera cher, malcommode, incertain et hors de la portée du citoyen qui ne pourra cacheter son courrier électronique (c'est le cas aujourd'hui).

Contrairement à ce que l'on considère comme naturel pour le téléphone et le courrier postal, le droit à avoir une correspondance privée n'existe donc pas sur les réseaux en France. Outre que la situation semble étonnante dans le pays des Droits de l'homme, une telle loi risque de pénaliser l'industrie française du logiciel et, d'une manière générale, toutes les firmes qui ont besoin de moyens sûrs pour protéger leurs communications.

Pourtant, si la loi gêne le citoyen honnête et la firme soucieuse de ses secrets, elle ne sert à rien contre ceux, qui pour des motifs inavouables, souhaitent communiquer discrètement avec des compères à l'autre bout du monde et qui utiliseront – et utilisent déjà aujourd'hui – des méthodes de stéganographie.

Remarquons aussi que l'évocation de l'usage d'*Internet* par la Mafia ou par les réseaux pédophiles semble aux yeux de certains justifier toutes les censures et interdictions. Pourtant, le problème posé n'est pas très différent de celui du téléphone : a-t-on interdit l'usage du téléphone parce que les cambrioleurs de banques ou les trafiquants d'enfants peuvent s'en aider pour monter leurs coups et organiser leurs trafics ?

J.-P. Delahaye

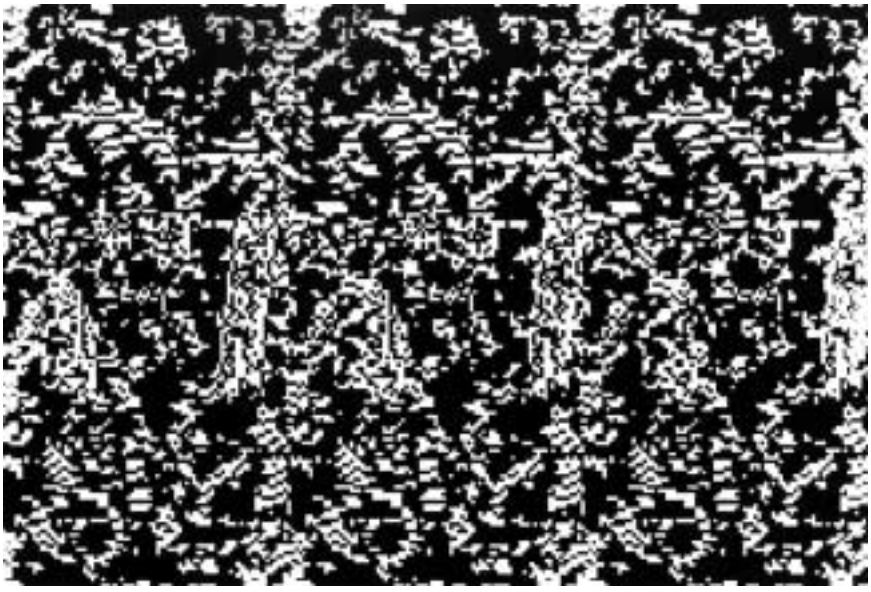
5. Vous convenez avec votre compère d'une liste de pixels. Par exemple, ceux dont les coordonnées sont des multiples de 20. Vous remplacez dans une image *a* les pixels de la liste par d'autres correspondant aux numéros des lettres du message secret que vous voulez transmettre. Ici les lettres du mot «stéganographie» ont été codées chacune sur 8 digits, ce qui fait 112 digits, qui ont été placés dans l'image aux points de coordonnées multiples de 20. Le «0» est codé par un point blanc, le «1» par un point noir. Votre compère qui recevra l'image *b* saura la déchiffrer et en tirer le message secret. Personne ne verra et ne saura qu'il y a eu quelque chose de caché. Cette méthode (dont il existe des versions plus perfectionnées) pour transmettre des messages secrets sans que personne puisse soupçonner qu'un message est transmis ne paraît pas pouvoir être détectée.

LES MONOSTÉRÉOGRAMMES

Un autre type de stéganographie utilisant les images a été l'objet d'une mode récente : les monostéréogrammes. La possibilité de cacher une forme tridimensionnelle dans une image à motifs répétitifs, en faisant varier insensiblement le motif répété, est une découverte extraordinaire et crée une situation assez amusante en matière de codage. Les méthodes pour créer les monostéréogrammes sont fondées sur des procédés algorithmiques programmés. En revanche, le décodage des monostéréogrammes nécessite toujours un être humain. Ce n'est peut-être pas irrémédiable, mais la situation mérite d'être notée : le codage est automatisé, le décodage non.

Ceux qui cherchent, parfois avec une ferveur quasi religieuse, des exemples de situations où l'homme est indubitablement supérieur à la machine et sont inquiets à propos de leur exemple favori (le jeu d'échecs), ou interprètent faussement les résultats d'indécidabilité de Gödel, devraient s'intéresser à ce cas étonnant.

Plus anciennes, mais dans la même veine picturale, les anamorphoses constituent une méthode de stéganographie qui a été pratiquée par de nombreux peintres : on ne découvre l'image cachée qu'en penchant le tableau ou en utilisant



J. Ninio

6. On a découvert récemment une nouvelle façon de cacher une image dans une autre. Pour voir l'image cachée (le mot «fin») : prenez l'image face à vous et collée contre votre nez et éloignez-la lentement : le relief va apparaître et le message. Patience. Ce stéréogramme a été mis au point par Jacques Ninio (ENS).

un miroir cylindrique. L'exemple le plus célèbre est celui du crâne caché dans le tableau de Hans Holbein *Les ambassadeurs*, peint en 1533.

QUELQUES RÉPONSES THÉORIQUES

L'idée qu'un message puisse comporter deux niveaux de lecture et même trois, comme nous l'avons évoqué à propos de la biologie, conduit à la question : est-il possible de créer des messages ayant une infinité de niveaux de lecture ? Que l'Univers soit un tel message est une idée qui nous amuse aujourd'hui, mais ne nous convainc pas, contrairement au Moyen Âge qui voyait des messages divins dans tous les objets du monde et trouvait séduisante cette perspective infinie de messages emboîtés. La théorie, par exemple, que chaque germe animal contient tous ses descendants enchâssés les uns dans les autres comme des poupées russes était communément admise, et en particulier fut défendue par Malebranche. Nous proposons de ramener le problème à une question mathématique précise.

Existe-t-il des messages infiniment profonds ? Pour simplifier le problème, imposons à la méthode de décodage d'être uniforme : pour lire le message de niveau n, on appliquera une méthode de décodage au message de niveau n – 1 et ce sera toujours la même méthode. La question rendue formelle est donc : «Peut-on créer une fonction de décodage f et un message infini M, tels que M, $f(M)$, $f(f(M))$, etc., soient des suites mathématiques intéressantes ?» (si l'on n'exigeait pas des suites obtenues d'être intéressantes, la réponse serait trivialement oui).

Il existe sans doute plusieurs façons de répondre à cette question, je vais juste en présenter une. Imposons au message de n'utiliser que des «0» et des «1», et à la méthode de décodage d'être celle qui transforme chaque paire de symboles «01» en «0» et chaque paire «10» en «1». Remarquez que cela entraîne que le message de base et les messages codés ne contiennent que des paires «01» et «10».

Les contraintes sont maintenant tellement fortes que notre problème ne comporte plus que deux solutions (la seconde s'obtient en inversant le rôle des 0 et des 1 dans la première). Un peu de réflexion ou la lecture de la figure 4 vous les feront trouver.

Une des contraintes du problème semble avoir été oubliée : comment est-on certain que les messages codés à chaque niveau sont intéressants, ainsi que l'énoncé du problème le stipulait ? La réponse rappellera le paradoxe du plus petit nombre inintéressant (qui ne peut exister, car sinon il serait intéressant du fait de sa définition) et elle consiste à dire : *(1)* d'abord le message est le même à chaque niveau (c'est facile à vérifier) et donc il suffit de montrer que chacune des deux solutions est une suite intéressante ; *(2)* puisqu'il n'y a que deux solutions (et donc une seule à une inversion près des 0 et des 1), elles constituent des suites mathématiques remarquables et donc intéressantes.

La suite de profondeur infinie trouvée comme solution de notre problème possède toutes sortes de propriétés remarquables. Elle s'appelle la suite de Prouhet-Thue-Morse et ne contient jamais trois fois consécutivement la même sous-séquence ; de plus, elle est stable lorsqu'on en enlève un élément sur deux (ce qui veut dire qu'une autre fonction de décodage que celle envisagée ci-dessus pourrait être utilisée) et c'est donc une sorte d'objet fractal : on la retrouve en elle-même en plus petit. Notons en passant que les objets fractals géométriques peuvent être vus comme des messages stéganographiques infiniment profonds se codant eux-mêmes.

LA STÉGANOGRAPHIE SUPERPURE ET DIEU

Toujours dans le domaine des mathématiques pures, Carl Sagan dans son roman *Contact*, dont le thème est la recherche d'intelligences extraterrestres envisageait un cas extraordinaire de stéganographie qu'on pourrait qualifier de «superpure» –, car le message anodin est le nombre π et ne contient donc rien d'arbitraire. En en calculant les décimales assez loin, Carl Sagan imagine qu'on finit par y découvrir de longues plages composées essentiellement de zéros qui, lorsqu'elles sont alignées les unes contre les autres, font apparaître un dessin de cercle parfait. Cette improbable stéganographie dans un texte fixé de toute éternité était interprétée comme la signature d'une intelligence ayant précédé l'Univers. Si un jour on trouve un message dans les décimales de π (ce qui ne s'est pas produit aujourd'hui), alors je crois, comme Carl Sagan, qu'on pourra effectivement y voir une preuve absolue de l'existence de Dieu. N'avais-je pas dit que la stéganographie était importante ?

J. NINIO, *Stéréomagie*, Éditions du Seuil, Paris, 1994.

J. BALTRUSAITIS, *Anamorphoses*, Flammarion, Paris, 1984.

H. BROCH, *Le paranormal*, Éditions du Seuil, Paris, 1985.

J. GUISNEL, *Guerres dans le cyberspace : services secrets et Internet*, La Découverte (Enquêtes), Paris, 1995.

D. R. HOFSTADTER, *Gödel, Escher, Bach ; les brins d'une guirlande éternelle*, Inter-Éditions, 1985.

D. KAHN, *La guerre des codes secrets : des hiéroglyphes à l'ordinateur*, Inter-Éditions, Paris 1980 (traduction de *The Codebreakers*, The Macmillan Company, New York, 1967).

B. SCHNEIER, *Cryptographie appliquée*, International Thomson Publishing, Paris, 1995.