LOGIQUE & CALCUL

La cryptographie visuelle

Une information cachée peut apparaître instantanément à notre œil qui, presque aussi bien qu'un ordinateur, l'extrait d'images grises.

Jean-Paul DELAHAYE

La moindre des qualités que doit posséder un homme d'honneur consiste à garder un secret. La plus grande consiste à oublier ce secret.
Al-Muhallab (672-720)

La cryptographie moderne propose des méthodes nouvelles et parfois extraordinaires pour cacher de l'information, puis, au prix de quelques calculs, pour la retrouver. L'ordinateur y joue un rôle central : le plus souvent, il n'est pas envisageable de s'en passer, ni pour chiffrer ni pour déchiffrer le message caché.

Il existe cependant une famille de procédés où l'ordinateur n'est pas obligatoire pour le déchiffrement. L'œil humain, associé à la puissance de calcul du système visuel de notre cerveau, sait opérer le calcul qui extrait un message clair de données aléatoires, et réussit l'opération avec une surprenante efficacité.

La « cryptographie visuelle » est le domaine spécialisé de la cryptographie qui s'occupe de développer et de perfectionner ce type de méthodes, nées en 1994 d'un travail de Moni Naor et Adi Shamir (le *S* du système de cryptage RSA).

La méthode de cryptographie visuelle de base est fondée sur le principe du « masque jetable ». Nous partons d'une image M (le masque) dont les pixels, uniquement noirs ou blancs, ont été tirés au hasard, et d'une image S de même taille, elle aussi composée uniquement de pixels noirs ou blancs, mais qui représentent le secret. L'image S, qu'on souhaite cacher et faire parvenir à un correspondant, peut être un dessin, une photo ou un texte, l'essentiel étant qu'elle soit de la même taille exactement que M et qu'elle ne comporte que des pixels noirs ou blancs.

Combiner le masque et le secret

À l'aide d'un logiciel de dessin ou d'un programme, on opère le « ou exclusif » (en informatique, on le note XOR) entre les pixels de M et ceux de S. Cela donne une image chiffrée C. En clair : pour chaque emplacement

1. La méthode du masque jetable

Les pixels du masque M *(a)* sont choisis aléatoirement, noir ou blanc. L'image secrète est S *(b)*. L'image chiffrée C *(c)*, de même taille que M, est calculée informatiquement en opérant un « ou exclusif », noté XOR, entre M et S : un pixel de C est blanc si les pixels de S et de M sont tous les deux blancs ou tous les deux noirs, sinon il est noir. L'image chiffrée C semble aléatoire, comme M.

La superposition d'un transparent sur lequel est imprimé M et d'un transparent sur lequel est imprimé C fait apparaître l'image secrète S plongée dans du « gris » *(d)*. L'œil a extrait l'information secrète. Cette superposition (M OU C) correspond à l'opération logique OU entre les deux images. Si l'on dispose de versions informatiques de M et de S, on peut opérer le OU EXCLUSIF (XOR) entre M et C, ce qui redonne parfaitement l'image secrète S *(e)*. Les lecteurs souhaitant disposer des images ci-contre sous forme de fichiers informatiques les trouveront en : http://www2.lifl.fr/~delahaye/PLS416.

a MASQUE : M

b IMAGE SECRÈTE : S

de pixel, si le pixel de M est le même que celui de S, on dessine sur C un pixel blanc, sinon on dessine un pixel noir. Le message chiffré C résulte ainsi d'un XOR entre le masque M et le secret S, c'est-à-dire C = M XOR S.

Après avoir créé les images M et C, si vous imprimez M et C sur des transparents, vous constaterez que la superposition de M et de C fait apparaître S. Si vous disposez d'un ordinateur, vous verrez encore mieux l'image S en opérant un XOR entre M et C *(voir l'encadré 1)*.

Voici maintenant comment utiliser ce procédé pour faire circuler des informations secrètes et les envoyer à quelqu'un ne disposant pas d'ordinateur, cela d'une manière parfaitement sûre.

Alain souhaite envoyer des messages secrets à Béatrice. Ils se rencontrent une première fois et produisent une série d'images aléatoires, les masques M_1, M_2, ..., M_n, dont ils gardent chacun une copie et que bien sûr personne d'autre ne devra connaître. Ils peuvent aussi convenir de ces masques secrets en les faisant circuler sur le réseau : Alain les crée et les envoie à Béatrice, ou l'inverse. Cependant, si on utilise le réseau, il faut être certain au moment de l'échange des images M_1, M_2, ..., M_n que personne d'autre n'en prend connaissance. C'est possible en utilisant un canal de communication protégé, ou en utilisant un procédé cryptographique tel que le RSA qui permet sans risque ce type de partages à distance.

Alain n'est pas prêt à noircir à la main pixel par pixel l'image chiffrée C ! Aussi dispose-t-il des masques sous la forme de fichiers informatiques et il utilise un ordinateur pour produire les images chiffrées C. Béatrice, elle, n'aura besoin de rien d'autre que ses yeux pour le déchiffrage. L'opération de partage des masques réalisée, Alain et Béatrice vont échanger des secrets en parfaite sécurité par la poste ou en utilisant des émissaires, même si ceux-ci peuvent être douteux.

Un masque à usage unique

Lorsque Alain souhaite communiquer à Béatrice une image secrète S, il choisit l'un des masques M_i dont il dispose ; il utilise son ordinateur pour calculer l'image $C = M_i$ XOR S qu'il poste ou fait remettre sous la forme d'un transparent à Béatrice en lui indiquant le numéro *i* du masque utilisé. Ce numéro *i* peut être inscrit sans risque sur le transparent, car celui qui ne dispose pas des transparents M_1, M_2, ..., M_n ne peut rien faire de l'information *i*, pas plus qu'il ne peut tirer quoi que ce soit du transparent C. Alain peut aussi transmettre l'image chiffrée C en utilisant le réseau et demander à Béatrice d'imprimer le transparent C quand elle reçoit le fichier numérique.

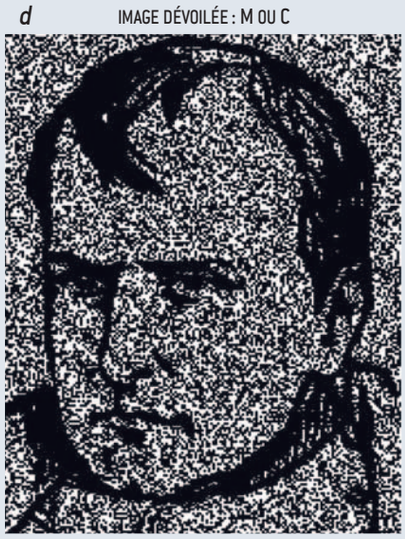
Pour que Béatrice prenne connaissance de l'image secrète, elle superpose le transparent reçu C et le transparent du masque M_i dont elle dispose. Alain et Béatrice jetteront le masque M_i qu'il ne faudra plus jamais utiliser.

Pour que la méthode résiste aux attaques d'espions, il est essentiel que les images des masques M_1, M_2, ..., M_n soient aussi aléatoires que possible : il faut les produire avec de bons procédés de génération de suites aléatoires et ne surtout pas prendre pour masques des images représentant quelque chose. De plus, il ne faut jamais réutiliser un masque M_i : si vous le faites, plus aucune garantie de confidentialité ne pourra être assurée *(voir l'encadré 2)*.

En respectant cette double consigne de sécurité, le procédé est sûr, car ce système cryptographique est équivalent à la méthode du masque jetable (aussi dénommé *one-time pad* ou code de Vernam), dont

c IMAGE CHIFFRÉE : C = M XOR S

d IMAGE DÉVOILÉE : M OU C



e IMAGE RECONSTITUÉE : M XOR C

2. Jamais deux fois le même masque !

a IMAGE SECRÈTE : S'

b IMAGE CHIFFRÉE : C' = M XOR S'

c IMAGE DÉVOILÉE : C OU C'

d IMAGE RECONSTITUÉE : C XOR C'

Si on utilise la méthode du masque jetable *(voir l'encadré 1)* pour créer des transparents chiffrés, il ne faut surtout pas utiliser deux fois le même masque. En voici la preuve.

Ici, en utilisant le même format d'image que pour l'encadré 1, et le même masque de chiffrage M, on a créé une image où est caché le mot SECRET, en opérant un XOR avec le masque M ; S' = SECRET *(a)*, C' = M XOR S' *(b)*. Un espion qui s'emparerait des deux messages secrets (celui avec la tête de Napoléon, et celui contenant le mot SECRET) et superposerait les transparents C et C' verrait l'image C OU C' *(c)*. Si l'espion opérait (à l'aide d'un ordinateur) un XOR entre les deux images chiffrées *(d)* soit C XOR C', ce qu'il obtiendrait serait encore plus net : car C XOR C' = (M XOR S) XOR (M XOR S') = S XOR 0 XOR S'= S XOR S'.

Utiliser un masque aléatoire une seule fois est une méthode inviolable, mais utiliser le même masque deux fois est une énorme bêtise.

L'AUTEUR

Jean-Paul DELAHAYE
est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

Claude Shannon a démontré l'absolue inviolabilité en 1949.

La superposition des deux transparents M_i et C fait bien apparaître l'image S, mais sous une forme dégradée (bruitée), car le OU opéré instantanément par l'œil laisse un bruit qui remplace le blanc de l'image secrète initiale. Si, au lieu d'utiliser l'œil, Béatrice dispose d'un ordinateur, un déchiffrage parfait est possible. En effet, nous savons que pour un message quelconque A, on a A XOR A = 0 et 0 XOR A = A (vous pouvez le vérifier avec les valeurs blanches et noires, blanc = 0, noir = 1) ; Béatrice opère un XOR entre M_i et C qui redonne S, car :
M_i XOR C = M_i XOR (M_i XOR S) =
(M_i XOR M_i) XOR S = 0 XOR S = S.

Insistons bien sur le fait qu'une fois le masque M_i et l'image chiffrée C créés, aucun des deux transparents à lui seul n'a la moindre information sur l'image secrète S. C'est évident pour M_i, puisqu'il a été créé sans même qu'on sache quelle serait l'image S qu'on chiffrerait. Voici maintenant le raisonnement qui montre que connaître C sans connaître M_i ne permet pas d'avoir la moindre information sur S.

Un espion qui dispose de l'image C et sait qu'elle a été engendrée par la méthode du masque jetable sans connaître le masque peut essayer tous les masques possibles qui, *a priori*, ont la même probabilité d'avoir été utilisés pour créer C à partir de S.

L'espion se dit qu'en essayant les masques systématiquement, quand il arrivera au bon M_i, il verra apparaître un dessin différent d'un nuage aléatoire, ce qui lui indiquera qu'il est en train d'utiliser le bon masque M_i. Cependant, cette idée est illusoire : pour toute image S' autre que S, il existe un masque M' qui, quand on l'applique à l'image chiffrée C en faisant un XOR, donne S' (il s'agit du masque M' = C XOR S'). En conséquence, en essayant systématiquement tous les masques possibles (ce qui par ailleurs n'est pas envisageable du fait de leur trop grand nombre), l'espion tombera sur une fausse solution S' avec la même probabilité que sur la véritable image secrète S. Cela étant vrai de n'importe quelle fausse solution S', pour celui qui n'a en main que C, il n'existe aucun moyen de distinguer S de n'importe quelle autre image S', et donc aucun moyen de

reconnaître que S est l'image qui a été cachée dans l'image chiffrée C.

La mise en œuvre de ce procédé est réellement facile. Pour réaliser les images de l'encadré 1, je n'ai utilisé aucun logiciel spécialisé : je me suis juste procuré des grilles aléatoires (en utilisant le logiciel *Golly*), puis j'ai réalisé les manipulations d'images avec un logiciel de dessin standard (*Graphic Converter* pour MacIntosh).

Information préservée

Cette méthode de base de la cryptographie visuelle a un petit défaut. Un pixel sur deux est perdu dans l'image M OU C, car si les pixels noirs de S sont bien retrouvés noirs, les pixels blancs sont, une fois sur deux, transformés en noir. Cette image M_i OU C est la seule que l'on voit si on ne dispose pas d'ordinateur pour opérer un XOR (qui, lui, redonne chaque pixel exactement). Si l'image S est suffisamment redondante, par exemple un texte écrit en assez grosses lettres, cela n'est pas ennuyeux. Cependant, si l'on souhaite transmettre à une personne sans ordinateur une image dont chaque pixel est important, la méthode du masque jetable ne conviendra pas. C'est sans doute pourquoi la méthode présentée par M. Naor et A. Shamir dans leur travail de 1994 est légèrement différente de la méthode de base.

En voici la description : chaque pixel de l'image à cacher est décomposé en deux demi-pixels ; de même pour les pixels des masques M_1, M_2, ..., M_n. Pour effectuer ces opérations sur des demi-pixels, on double la taille de l'image, ce qui fait que chaque groupe de quatre pixels peut être

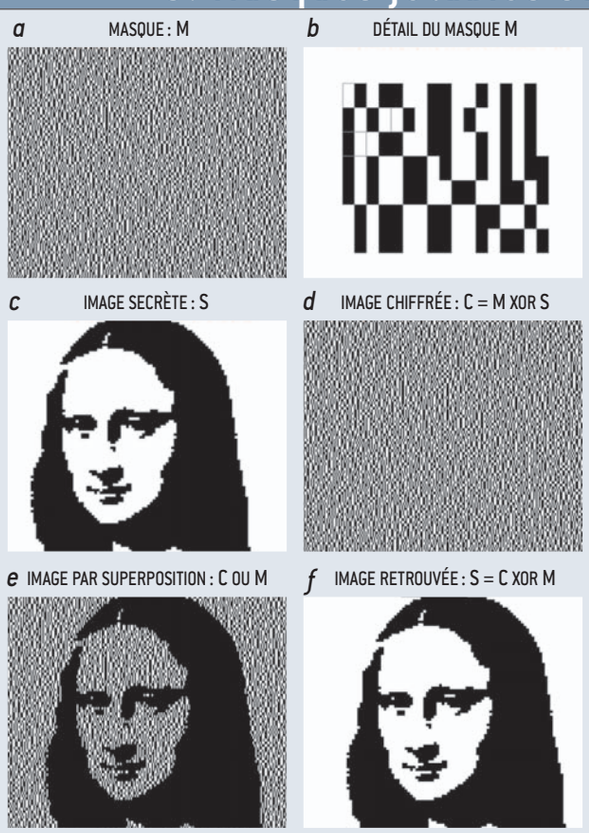
✔ BIBLIOGRAPHIE

S. Cimato et C.-N. Yang, **Visual Cryptography and Secret Image Sharing**, CRC Press Inc., 2011.

Visual cryptography, *Wikipedia* (consulté en mars 2012) : http://en.wikipedia.org/wiki/Visual_cryptography

M. Naor et A. Shamir, **Visual Cryptography**, *EUROCRYPT 1994*, pp. 1-12 : www.wisdom.weizmann.ac.il/~naor/PUZZLES/visual_sol.html

3. Masques jetables sans perte d'information



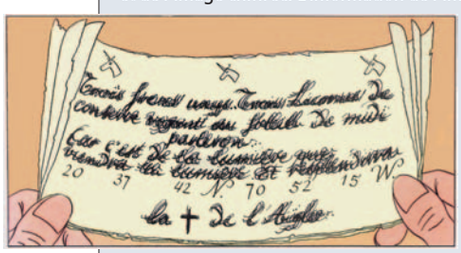
La première méthode a un défaut : l'image reconstituée à l'œil par superposition du masque M et de l'image chiffrée S (qui correspond à un OU et non à un XOR) ne redonne pas tous les pixels blancs, mais en transforme un sur deux en pixel noir. En coupant chaque pixel en deux (un côté droit et un côté gauche), on évite cette perte d'information due à l'utilisation d'un OU plutôt que d'un XOR (opération que l'œil ne sait pas faire !).

On part maintenant d'un masque M *(a)* constitué de pixels découpés en deux : on a doublé la taille de l'image pour que chaque pixel de base soit maintenant composé d'un carré de quatre pixels. Soit la moitié droite, soit la moitié gauche de chaque « gros pixel » sera noire, ce choix étant opéré aléatoirement *(détail en b)*.

L'image chiffrée C *(c)* est obtenue en opérant un XOR entre l'image secrète S (dont on a doublé la taille) et le masque M, ce qui inverse les pixels du masque correspondant à des pixels noirs de S :
– si le pixel du masque est noir du côté droit et que le pixel correspondant de S est noir, alors le pixel de C sera noir du côté gauche (et inversement) ;
– si le pixel de l'image secrète S est blanc, le pixel de l'image chiffrée sera le même que celui du masque.

La reconstitution de l'image secrète se fait comme auparavant. On obtient, en superposant les images M et C (c'est-à-dire en faisant M OU C), une image où les pixels noirs de S sont noirs, et où les pixels blancs de S sont remplacés par des pixels à moitié noirs (à droite ou à gauche aléatoirement). Aucune information n'est perdue. Comme précédemment, en opérant un XOR entre M et C (ce qui exige un ordinateur et non pas seulement deux transparents), on reconstitue exactement et avec le contraste initial l'image secrète S.

4. Éclatement d'une image en trois



Pour reconstruire les informations de l'image dans les deux méthodes décrites dans le texte de l'article, il faut disposer à la fois du masque et de l'image chiffrée. L'information de l'image a été éclatée en deux. On peut faire mieux et éclater une image en trois morceaux (ou plus) dont aucun à lui seul n'indiquera rien à propos de l'image secrète S, et dont même la possession de deux des trois images ne permettra pas de tirer la moindre information sur S. Celui qui n'a pas les trois images n'a rien ! Si Hergé, dans *Le secret de la licorne,* avait connu ce procédé, il l'aurait certainement retenu pour les trois parchemins cachés *(voir l'image ci-dessus),* dont la superposition indique l'emplacement de l'épave au trésor.

Voyons le procédé permettant l'éclatement parfait d'une image en trois images. On divise d'abord chaque pixel en quatre sous-pixels.

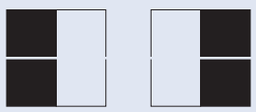
Si l'image secrète est de taille $n \times m$, on va créer trois images A, B et C, chacune de taille $2n \times 2m$, dont la superposition fera apparaître l'image secrète S. À la place des pixels blancs, la superposition de A, B et C montrera des pixels 2×2 comportant chacun un sous-pixel blanc et trois sous-pixels noirs, et à la place des pixels noirs la superposition comportera des pixels 2×2 entièrement noirs. Malgré une importante perte de contraste, l'information sera donc complètement restituée par la superposition de A, B et C (et un traitement informatique redonnerait exactement S).

L'image A *(voir ci-dessous)* sera composée de pixels 2×2 choisis aléatoirement (NB, NB) ou (BN, BN). L'image B sera composée de pixels 2×2 choisis aléatoirement parmi (BB, NN) ou (NN, BB). L'image C sera composée de pixels 2×2 choisis parmi (BN, NB) ou (NB, BN). Les pixels de C ne seront pas choisis aléatoirement, mais de façon que :

– si le pixel correspondant de l'image secrète S est blanc, alors la superposition des pixels correspondants de A, B et C comportera un sous-pixel blanc et trois noirs ;

– sinon, la superposition de A, B et C sera composée de quatre sous-pixels noirs.

On vérifie facilement qu'une telle transformation est toujours possible en considérant les quatre cas possibles pour un pixel de A et un pixel de B.



Pixels de A (NB,NB) ou (BN,BN)

Pixels de B (BB,NN) ou (NN,BB)

Pixels de C (BN,NB) ou (NB,BN)

Montrons que ce procédé a bien les propriétés annoncées : connaître deux des trois images A, B et C ne donne aucune information sur l'image secrète S. Il est clair que celui qui dispose de A et de B n'a aucune information sur l'image secrète S, car A et B ont été tirées au hasard sans même utiliser S.

Montrons que, de même, disposer de A et C ne donne rien concernant S (le raisonnement sera le même avec B et C). Considérons un pixel de S de coordonnées (x, y). Les pixels correspondants de A et C recouvrent exactement trois des quatre sous-pixels (on le vérifie en considérant les quatre cas possibles). Selon que le pixel correspondant de B est noir en haut ou en bas, le pixel de la superposition de A, B et C représentera un pixel blanc de S ou un pixel noir. Ne pas avoir B implique donc qu'on n'a aucune information sur ce pixel (x, y) de S. Cela étant vrai pour tout pixel de S, celui qui dispose uniquement de A et C ne sait absolument rien de S.

On constate qu'en superposant deux des trois images A, B ou C, aucune information n'apparaît.

IMAGE SECRÈTE S

IMAGE A

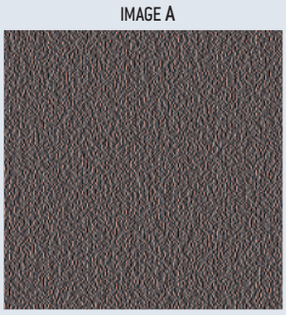


IMAGE B

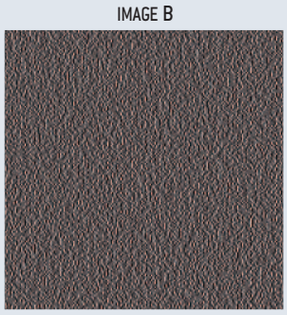


IMAGE C

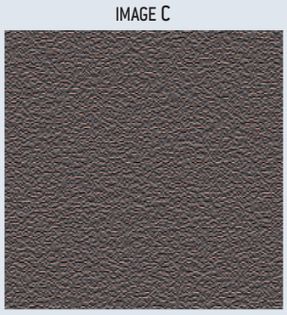


IMAGE (A OU B OU C)

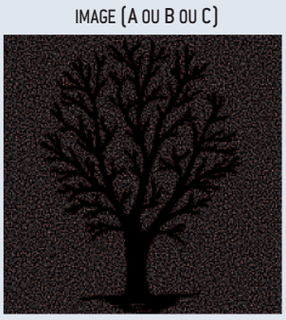


IMAGE (A OU B)

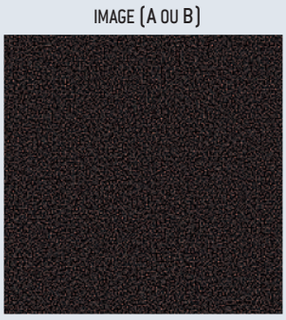


IMAGE (B OU C)

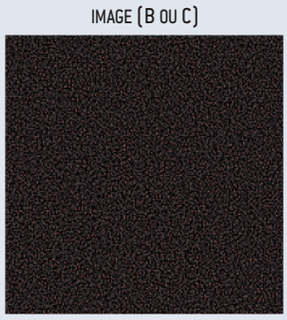
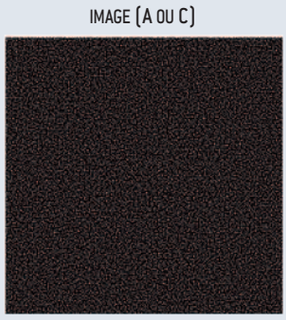


IMAGE (A OU C)



considéré comme un seul pixel et est maintenant séparable en deux (et même en quatre, ce qui sera utile pour d'autres procédés de chiffrage).

Les images M_1, M_2, ..., M_n sont constituées cette fois d'une grille aléatoire de demi-pixels : selon un tirage aléatoire aussi parfait que possible, chaque pixel de M_i est rempli par un demi-pixel droit noir ou un demi-pixel gauche noir, ou l'inverse.

L'image chiffrée C est elle aussi composée de demi-pixels. Le demi-pixel en position (x, y) de C sera identique à celui du masque M_i si le pixel de l'image secrète S en position (x, y) est blanc et sera le demi-pixel complémentaire de celui de M_i sinon. Comme précédemment, les images M_i ou l'image C sont d'un gris uniforme et aucune ne contient la moindre information sur S *(voir l'encadré 3)*.

Lorsque l'on superposera C et M_i, là où il y a un pixel noir dans S, on aura un pixel noir, et là où il y a un pixel blanc, on aura un demi-pixel noir et un demi-pixel blanc (puisque ceux de C et de M_i auront été choisis identiques).

Cette fois, l'observation de la superposition opérée par l'œil redonne tous les pixels de S. La présence de demi-pixels là où il y avait des blancs a pour effet de changer le contraste (le blanc est devenu gris), mais aucune information n'est perdue dans l'image M_i OU C qui, cette fois, reconstitue parfaitement l'image secrète S, au contraste près *(voir l'encadré 3)*.

Perfectionnements... et une énigme

L'idée de découper un pixel en sous-pixels permet d'autres miracles, dont voici deux exemples.

Éclatement d'une image en *m* morceaux

Pour tous entiers positifs *k* et *m* donnés, on peut définir un système de construction de transparents tel que l'image secrète S donnera *m* images chiffrées C_1, C_2, ... C_m différentes et telles que la connaissance de moins de *k* d'entre elles ne permet pas de connaître quoi que ce soit de l'image secrète S, alors que la connaissance de *k* images parmi C_1, C_2, ..., C_m, quelles qu'elles soient, permet de reconstituer l'image S.

Autrement dit, une fois les informations de S éclatées en C_1, C_2, ..., C_m et distribuées à *m* personnes différentes, si *k* d'entre elles se mettent d'accord, elles peuvent retrouver S, mais si elles sont moins de *k*, elles n'en tireront strictement rien.

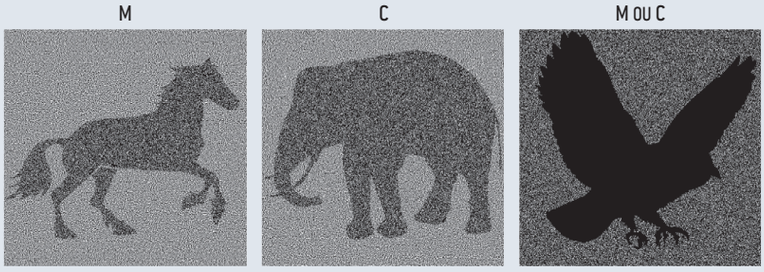
Une méthode d'éclatement d'une image secrète en trois transparents C_1, C_2, C_3 tels que deux parmi les trois transparents ne donnent absolument rien de S, mais telle que la superposition des trois redonne S est décrite dans l'encadré 4 et présentée avec un exemple.

Le secret insoupçonnable

La méthode produit deux images, chacune d'apparence innocente U et V (par exemple un cheval et un éléphant). Cependant, la superposition de U et de V fait disparaître ce qu'il y avait sur U et V et fait apparaître une troisième image, celle secrète qu'on avait cachée *(voir l'encadré 5)*.

Pour terminer, nous vous invitons à consulter l'encadré 6 ci-contre, qui propose une petite énigme cryptographique. ■

5. Masques imagés

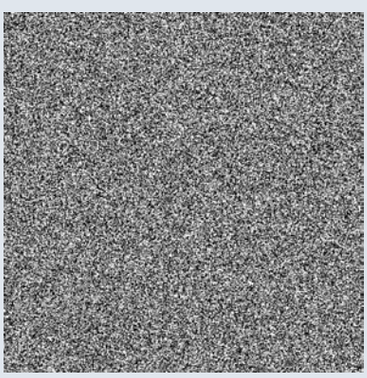


Les méthodes décrites dans les encadrés 1, 2, 3 et 4 risquent d'attirer les soupçons si vous les utilisez, car on se doutera que les images grises « d'allure aléatoire » portent une information cachée. C'est pourquoi un perfectionnement a été proposé : le masque M aussi bien que l'image chiffrée C ne sont plus gris, mais représentent des images ayant un intérêt en soi. La superposition des deux fait disparaître les deux images initiales et fait apparaître l'image secrète.

Nous n'indiquons pas le détail du procédé qu'un peu de réflexion vous fera imaginer.

On remarquera que dans les deux images M et C, le dessin est obtenu avec deux types de gris : un gris 50 % (moitié pixels blancs, moitié pixels noirs) et un gris 75 % (1/4 de pixels blancs, 3/4 de pixels noirs), alors que dans l'image reconstituée de S, il y a deux types de gris : un gris 75 % et un gris composé de 100 % de pixels noirs, qui permet de voir très clairement l'image secrète.

6. Énigme



Cette image contient un message caché (le prénom d'un mathématicien) par un procédé proche de ceux évoqués dans l'article. Le découvrir ne demande aucun programme particulier, juste un peu d'astuce. Comme pour les autres images de cet article, vous trouverez une version numérique de cette image en :
http://www2.lifl.fr/~delahaye/PLS416.

La première personne à me communiquer la bonne réponse par courriel à l'adresse delahaye@lifl.fr gagnera un abonnement d'un an à *Pour la Science*.