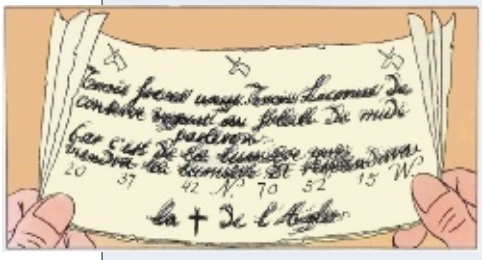
4. Éclatement d'une image en trois



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.

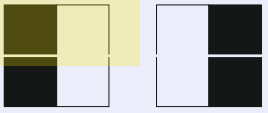
Si l'image secrète est de taille $n \times m$, on va créer trois images A, B et C, chacune de taille $2n \times 2m$, dont la superposition fera apparaître l'image secrète S. À la place des pixels blancs, la superposition de A, B et C montrera des pixels 2×2 comportant chacun un sous-pixel blanc et trois 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 ;

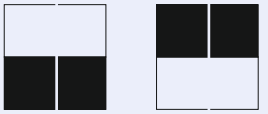
– sinon, la superposition de A, B et C sera composée de quatre sous-pixels noirs.

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)

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.



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

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.

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

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

IMAGE SECRÈTE S

IMAGE A

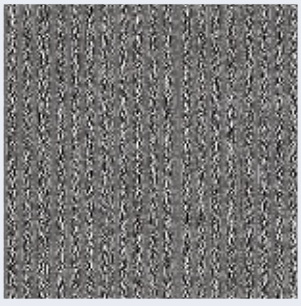


IMAGE B

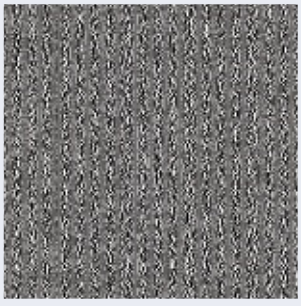


IMAGE C

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

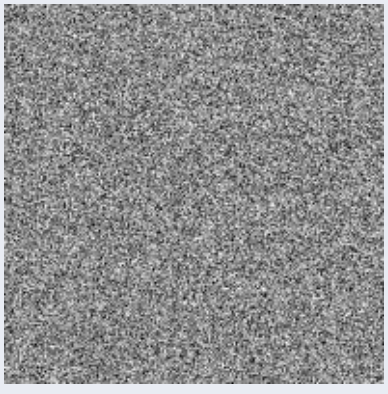
M | C | M OU C

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*.