

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

Les images $M_1, M_2, \dots, M_n$ 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).

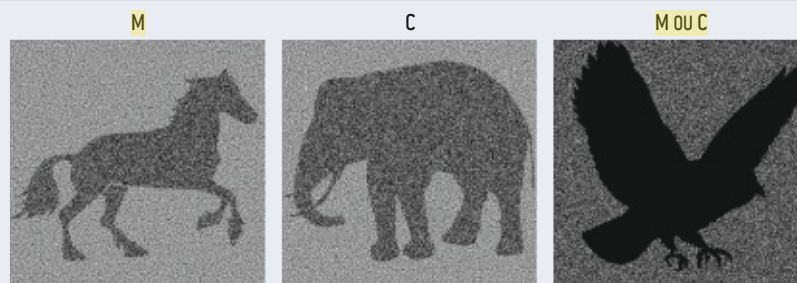
Perfectionnements... et une énigme

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 $C_1, C_2, \dots, C_m$ 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

5. Masques imagés

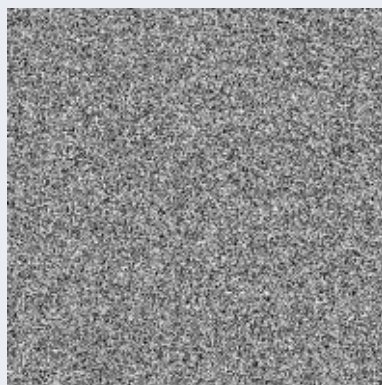


Les méthodes décrites dans les encadrés 1, 2, 3 et 4 risquent d'attirer les soupçons si vous les utilisez, car on se doutera que les images grises « d'allure aléatoire » portent une information cachée. C'est pourquoi un perfectionnement a été proposé : le masque M aussi bien que l'image chiffrée C ne 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*.

connaissance de k images parmi $C_1, C_2, \dots, C_m$, quelles qu'elles soient, permet de reconstituer l'image S .

Autrement dit, une fois les informations de Séclatées en $C_1, C_2, \dots, C_m$ 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. ■