par P. Lafourcade, C. Lauradoux et M. More

Initiation à la cryptographie visuelle

La cryptographie permet de chiffrer des messages afin d'établir des communications sécurisées. Ils ne peuvent alors être déchiffrés que par les personnes connaissant une clé secrète. Des techniques basées sur la décomposition de pixels permettent de chiffrer des messages.

Une séance. Groupes de deux élèves.
Tous niveaux à partir du cycle 2.

Objectifs :

- découvrir la cryptographie visuelle ;
- réfléchir à la sécurité des données.

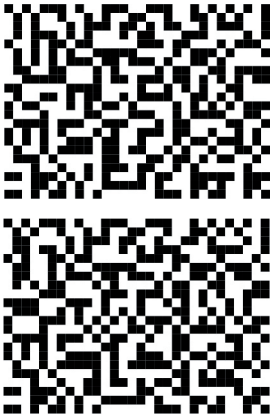
Compétences travaillées :

- comprendre le mécanisme de la cryptographie visuelle ;
- déchiffrer une image chiffrée avec une clé secrète partagée ;
- générer une clé secrète et chiffrer une image.

Communiquer des informations sensibles en toute sécurité est l'objectif de la cryptographie. Cette activité vise à faire découvrir la *cryptographie visuelle*, inventée par les mathématiciens Moni Naor (né en 1961) et Adi Shamir (né en 1952) et présentée en 1994 au congrès Eurocrypt'94. Cette technique permet de chiffrer et de déchiffrer des images constituées de pixels.

Le principe de la cryptographie visuelle

Les deux images ci-dessous sont à imprimer en assez grande taille sur une feuille blanche pas trop épaisse (voir en annexe page 72). Elles sont proposées aux élèves, en leur expliquant seulement qu'elles cachent un secret.

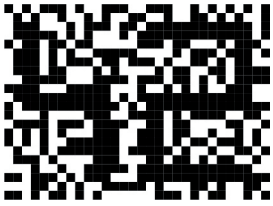


L'objectif est qu'ils découvrent par eux-mêmes le fonctionnement de la cryptographie visuelle. Ces images sont constituées de pixels noirs et blancs dont

la disposition semble *a priori* aléatoire. Les élèvent manipulent ces images de diverses façons, jusqu'à trouver celle qui fait apparaître une image secrète.

En observant les images, ils finissent par s'apercevoir qu'elles ont de nombreux pixels identiques, mais pas tous. Pour mieux visualiser les différences, il est possible de colorier sur l'une les pixels qui sont différents sur l'autre, ou encore de les superposer par transparence devant une fenêtre ou une lampe.

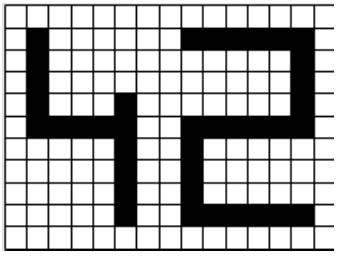
La superposition des deux images fait apparaître l'image secrète suivante :



Elle est un peu brouillée, mais l'œil humain n'a aucune difficulté à extraire l'information qu'elle contient, au besoin en s'éloignant un peu. En revanche, une personne qui n'a qu'une seule des deux images ne peut pas découvrir l'image secrète, ni même obtenir d'information à son propos.
Lorsqu'il s'agit de communiquer une image secrète, l'une des deux images est une *clé secrète* partagée au préalable entre les deux correspondants, et l'autre est l'*image chiffrée* proprement dite, que l'expéditeur fait parvenir au destinataire. La clé secrète sert, pour l'expéditeur, à générer l'image chiffrée à partir d'une image en clair et, pour le destinataire, à la déchiffrer.

Chiffrer une image

Partant d'une image, l'objectif est de générer deux images qui semblent aléatoires, et qui révèlent l'image originelle une fois superposées. L'idée de Naor et Shamir est de transformer chaque pixel de l'image de départ en quatre pixels. Ainsi, les deux images obtenues (respectivement la clé secrète et l'image chiffrée) seront quatre fois plus grandes, en nombre de pixels, que l'image d'origine.
Par exemple, l'image de départ était la suivante :



Chaque pixel sur l'image en clair produit quatre pixels, organisés en carré, à la fois sur la clé secrète et sur l'image chiffrée.

© Pascal Lafourcade

par P. Lafourcade, C. Lauradoux et M. More

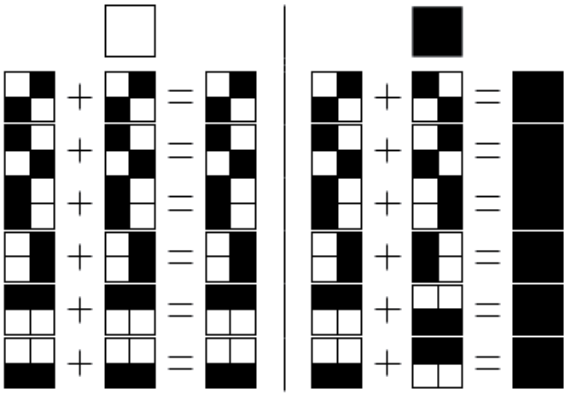


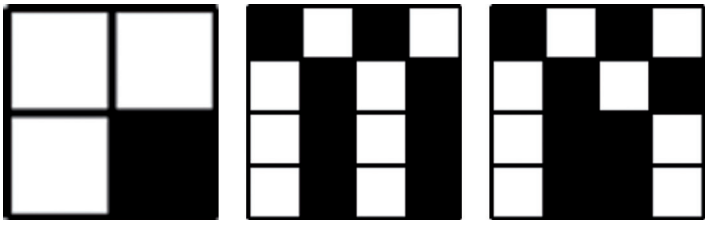
Tableau de chiffrement. Chaque pixel original est codé aléatoirement par deux ensembles de quatre pixels (deux blancs et deux noirs). Si les deux ensembles sont identiques, on a affaire à un pixel blanc. Si les deux ensembles sont complémentaires, il s'agit d'un pixel noir.

Plus précisément, pour chaque pixel blanc de l'image en clair, une règle parmi les six du tableau (à gauche) est choisie aléatoirement, et l'un des carrés est reproduit sur la clé, l'autre sur l'image chiffrée. Ainsi en superposant les deux images obtenues, un pixel blanc de l'image initiale correspond à un bloc de quatre pixels à moitié blancs et identique sur les deux images.
Pour un pixel noir, il faut choisir, de manière aléatoire, deux carrés complémentaires parmi les six règles du tableau (à droite). Le carré de quatre pixels obtenu en les superposant est alors entièrement noir.

Lorsque la clé secrète est construite au préalable et partagée entre les correspondants, cela revient à fixer d'avance la ligne choisie dans le tableau de chiffrement, pour chaque pixel de l'image en clair. Le schéma de gauche est alors représenté sur la clé, tandis que l'un des deux schémas de droite sera reproduit sur l'image chiffrée au moment du chiffrement, en fonction de la couleur du pixel de l'image en clair.

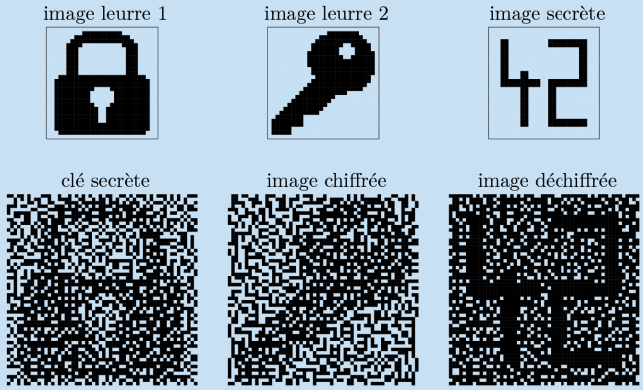
Ces règles ont pour objectif de produire une clé secrète et une image chiffrée contenant chacune autant de pixels noirs que de pixels blancs, disposés d'une manière qui semble aléatoire sur chaque image séparément. Ainsi, une image seule ne permet de retrouver aucune information sur l'image secrète. En effet, comme les règles de génération des images sont choisies aléatoirement, un adversaire n'ayant accès qu'à l'image chiffrée et non à la clé secrète (ou le contraire) n'est pas capable de savoir si la superposition donnera un bloc à moitié noir ou un bloc entièrement noir.
Suivant le temps dont on dispose et leur niveau, on pourra demander aux élèves, après avoir trouvé le dessin secret, de découvrir également le procédé de chiffrement (on leur fournira pour cela l'image originale, en plus des deux premières).

Un exemple de codage : le premier dessin est l'image originale, le deuxième est la clé secrète. Pour obtenir l'image chiffrée (à droite), les blocs 4×4 correspondant aux trois pixels blancs sont reproduits à l'identique. Le dernier bloc est inversé.

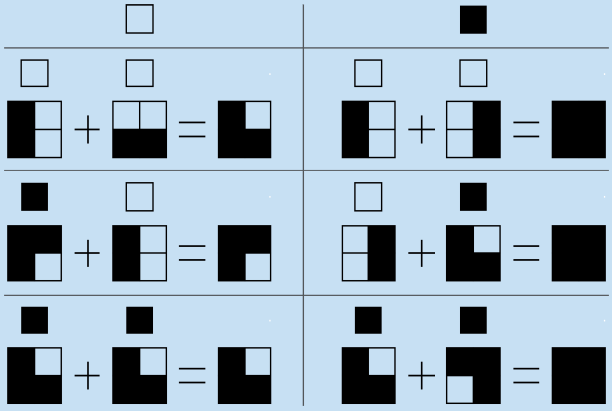


Des images leurres

Une variante intéressante du procédé de cryptographie visuelle implique l'utilisation d'images leurres : la clé secrète et l'image chiffrée ne sont alors pas aléatoires, mais elles correspondent elles-mêmes à des images. Il y a dans ce cas trois images de départ : deux images leurres et une image secrète, toutes de même dimension. Sur la clé comme sur l'image secrète, le dessin de l'une des images leurres est reconnaissable et, en les superposant, c'est l'image secrète qui apparaît, comme illustré ci-dessous.



Comme précédemment, la clé secrète et l'image chiffrée sont générées de manière aléatoire. Mais au lieu d'avoir un tableau de codage, on en utilise trois, suivant les couleurs des pixels correspondants sur les deux images leurres (tous les deux noirs, tous les deux blancs, deux couleurs différentes). L'emploi des blocs de trois pixels noirs rend possible cette multiplication des choix possibles. Avec ce processus, les blocs de l'image déchiffrée correspondant à des pixels blancs sont à 75 % noirs (au lieu de 50 %, comme dans le texte).



Chaque ligne correspond ici à un seul exemple pris dans chacun des trois tableaux de codage. Saurez-vous déterminer le nombre total de possibilités dans chaque cas ?

par P. Lafourcade, C. Lauradoux et M. More

S'échanger des images chiffrées

Maintenant qu'ils ont compris le principe de cryptographie visuelle, la seconde partie de l'activité consiste, pour chaque binôme, à créer, en commun, une clé secrète partagée et, chacun, une image chiffrée à partir d'un dessin de leur choix.

Pour cela, chacun commence par dessiner de son côté une image secrète « en *pixel art* » (en noir et blanc, de la même taille $n \times p$). Ensuite, les deux élèves se mettent d'accord sur une clé secrète partagée de $2n$ lignes de $2p$ pixels en choisissant aléatoirement des blocs de quatre pixels parmi les six possibilités. Chacun utilise alors un calque pour générer son image chiffrée : pour chaque pixel de son image secrète, il suffit de colorier les mêmes pixels (si c'est blanc) que sur la clé, ou les pixels complémentaires (si c'est noir). Un exemple d'une réalisation 5×3 est donnée en annexe en page 72.

Une fois que chaque élève d'un binôme a terminé de créer son image chiffrée, ils se les échangent. Ainsi, chacun est capable de superposer la clé partagée et l'image chiffrée de son camarade pour découvrir l'image secrète de ce dernier. La taille des images utilisées permet de s'adapter à l'âge et à la patience des élèves. Une autre possibilité est de choisir une image secrète plus grande et de diviser le travail entre plusieurs élèves.

P. L., C. L. & M. M.

© Pascal Lafourcade

Référence

25 énigmes ludiques pour s'initier à la cryptographie, Pascal Lafourcade et Malika More. Dunod, 2021.

ADAPTATION

- Pour adapter l'activité à différents publics, un générateur en ligne (**sancy.iut.uca.fr/~lafourcade/Cryptovisuelle**) permet de créer des images en pixel art de différentes tailles, mais aussi de téléverser ses propres images aux formats JPEG et PNG, de générer des images chiffrées en différents formats et des GIF animés montrant le déchiffrement. Il permet aussi de générer des exemples pour la variante utilisant des images leurres.
- Pour des lycéens, il est envisageable de coder les algorithmes de chiffrement, de déchiffrement et de génération des clés, ainsi qu'un algorithme de « nettoyage » d'une image déchiffrée, transformant les groupes de pixels à moitié noirs en pixels blancs.
- Pour les plus jeunes, cette activité peut intervenir à la fin de plusieurs séances sur les images pixelisées, une fois que les élèves en connaissent bien le principe (voir *Les codes de la télévision*, Maryline Althuser, *Tangente Éducation* 42-43, 2017).