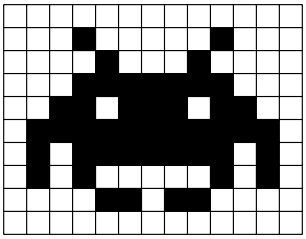
décembre 2023

Cryptographie visuelle

L'objectif de ce document est de présenter deux activités à réaliser en classe pour découvrir la cryptographie visuelle.

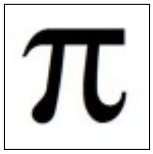
1 Présentation

La cryptographie visuelle a été inventée en 1994 par Moni Naor et Adi Shamir (voir [1]). Elle permet de **communiquer des messages secrets à travers des images**. Nous allons manipuler des images simples en noir et blanc. Elles sont donc constituées uniquement de **pixels** noirs ou blancs. Dessiner avec des pixels est utilisé de nos jours par ceux qui se servent de *post-its* pour faire du *pixel art*. Ci-dessous un exemple de dessin en pixels représentant un monstre de *Space Invaders*.

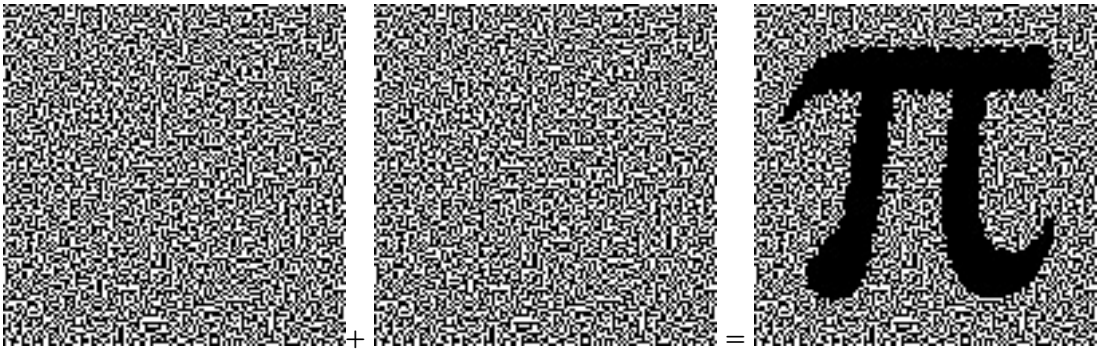


Principe de la cryptographie visuelle L'idée est de construire deux images de telle sorte qu'en les superposant elles font apparaître le message secret. Mais une personne qui ne possède qu'une seule image ne doit pas pouvoir retrouver le message secret. Elle ne doit pouvoir obtenir aucune information sur le message secret avec une seule des deux images. La méthode de construction des deux images est détaillée dans le paragraphe suivant.

Exemple En partant de l'image originale représentant le symbole π



Nous obtenons les deux images suivantes qui, en fusionnant donnent la troisième image.



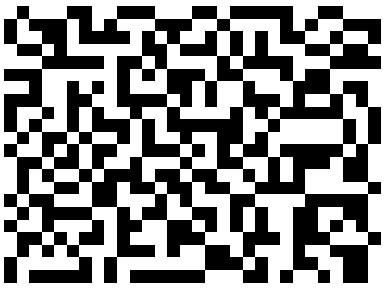
Nous remarquons que le la partie blanche ne l'est plus. L'image finale ne sera pas exactement celle de départ. Elle sera moins « nette ».

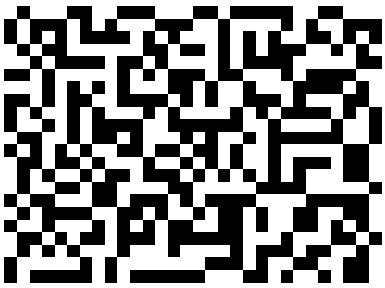
2 Mise en œuvre

Nous détaillons dans ce paragraphe deux activités pour découvrir puis mettre en œuvre la cryptographie visuelle dans la classe.

2.1 Découverte de la cryptographie visuelle.

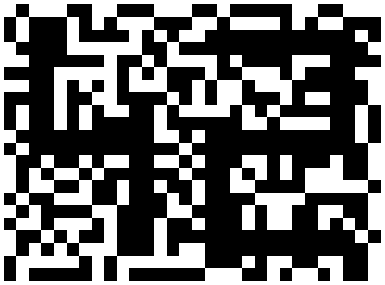
Les deux images ci-dessous, imprimées en assez grande taille sur une feuille blanche pas trop épaisse, sont proposées aux élèves en leur expliquant seulement qu'elles cachent un secret. L'objectif est qu'ils découvrent par eux-mêmes le fonctionnement de la cryptographie visuelle. Ces images sont constituées de pixels noirs et blancs et semblent a priori aléatoires. Les élèvent doivent manipuler ces images de diverses façons, jusqu'à trouver celle qui fait apparaître une image secrète.





Solution. En observant les images, les élèves 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 des images les pixels qui sont différents sur l'autre, ou encore de superposer les images par transparence devant une fenêtre ou une lampe.

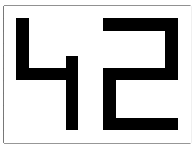
La superposition des deux images fait apparaître l'image secrète suivante :



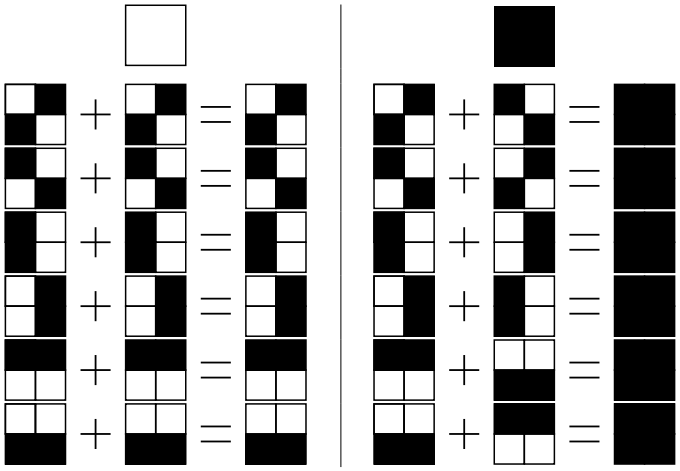
Elle est un peu brouillée, mais l'oeil humain n'a aucune difficulté à déterminer l'information qu'elle contient, au besoin en s'éloignant un peu. En revanche, une personne qui n'a qu'une seule des deux images ne peut pas découvrir l'image secrète, ni même obtenir aucune information à son propos.

L'enseignant peut alors expliquer que, lorsque cette technique est utilisée pour échanger des images secrètes, 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 à l'expéditeur à générer l'image chiffrée à partir d'une image en clair, et aussi au destinataire pour la déchiffrer.

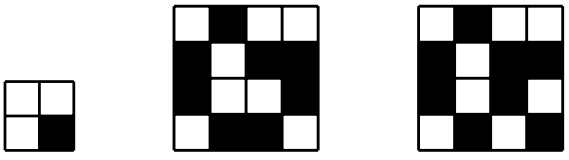
Fonctionnement de l'algorithme de chiffrement. Partant d'une image, il faut générer deux images qui semblent aléatoires, et qui révèlent l'image originelle quand elles sont superposées. L'idée de Noar et Shamir est de transformer chaque pixel de l'image de départ en quatre pixels. Ainsi, les deux images 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. Plus précisément, rappelons que, pour chaque pixel blanc de l'image en clair, une règle parmi les 6 suivantes à gauche est choisie aléatoirement, et l'un des carrés est écrit 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. Pour un pixel noir, il faut choisir, de manière aléatoire, deux carrés complémentaires parmi les 6 règles ci-dessous 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 parmi les règles ci-dessus, pour chaque pixel de l'image en clair. Le schéma de gauche est alors écrit sur la clé, tandis que l'un des deux schémas de droite est écrit sur l'image chiffrée au moment du chiffrement en fonction de la valeur du pixel de l'image en clair. Ainsi, pour les 4 pixels en haut à gauche de l'image initiale, les règles des lignes 1, 6, 2 et 1 ont été choisies, ce qui donne les 16 pixels en haut à gauche pour la clé secrète et l'image chiffrée respectivement, comme illustré ci-dessous :



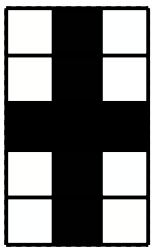
Comment être sûr que la sécurité est garantie ? Les règles ont pour objectif de produire une clé secrète et une image chiffrée qui contiennent chacune autant de pixels noirs que de pixels blancs, disposés d'une manière qui semble aléatoire sur chaque image séparément. Ainsi, une image seule ne permet 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 permet d'obtenir un bloc à moitié blanc ou un bloc entièrement noir.

Un prolongement intéressant pour les lycéens peut être de constater que si une même clé secrète est utilisée pour chiffrer plusieurs images, la sécurité n'est plus assurée. Par exemple, imaginons chiffrer un grand disque noir sur fond blanc d'une part, et un petit carré blanc sur fond noir d'autre part, sans changer la clé secrète. En superposant les deux images chiffrées, l'extérieur du disque et l'intérieur du carré apparaissent en noir, et l'intérieur du disque en noir

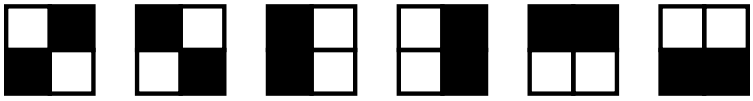
et blanc mélangés. Autrement dit, des informations sur les images secrètes peuvent être obtenues sans disposer de la clé ! Ce n'est pas très difficile à démontrer en examinant les différents cas possibles.

2.2 Générer une clé secrète partagée et chiffrer/déchiffrer une image.

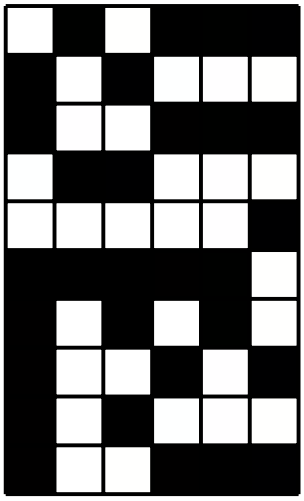
Lorsque l'algorithme de chiffrement est bien compris, les élèves de chaque binôme vont créer une clé secrète partagée et une image chiffrée chacun à partir d'une image de leur choix. Pour cela, ils se mettent par deux et chacun commence par dessiner de son côté une image secrète en pixel art en noir et blanc de la même taille. Par exemple, l'image ci-dessous, composée de 5 lignes de 3 pixels, représente le symbole +.



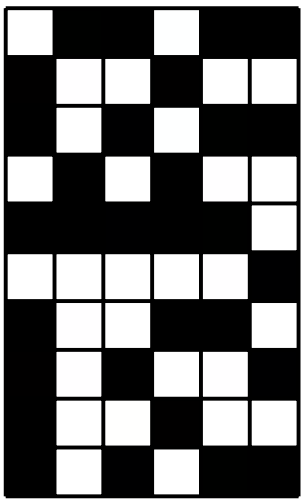
Ensuite, les deux élèves se mettent d'accord sur une clé secrète partagée de 10 lignes de 6 pixels en choisissant aléatoirement des blocs de 4 pixels parmi les 6 possibilités suivantes :



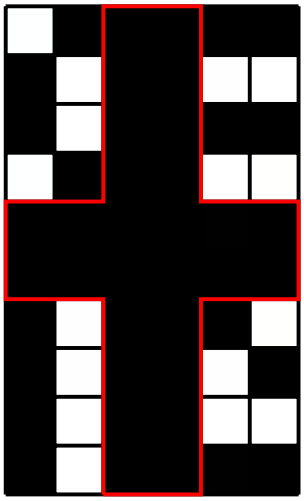
Par exemple, une clé secrète partagée possible est :



Ensuite, chacun utilise 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). Par exemple, l'élève qui a dessiné la croix obtiendra comme image chiffrée :



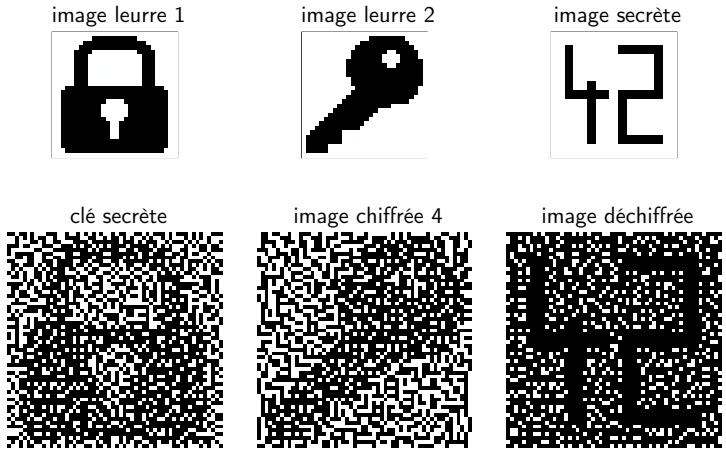
Une fois que chaque élève d'un binôme a fini de créer son image chiffrée, ils se les échangent. Ainsi, chacun est capable de superposer leur clé partagée et l'image chiffrée de son camarade pour découvrir l'image secrète de celui-ci. En continuant notre exemple, la superposition de la clé et d'image chiffrée laisse apparaître l'image déchiffrée suivante, sur laquelle la croix est entourée d'un trait rouge pour faciliter la lecture :



En effet, avec aussi peu de pixel au départ, l'image déchiffrée est extrêmement bruitée, mais la perte de contraste observée est inhérente à la méthode de chiffrement, puisque les pixels initialement blancs sont remplacés par des groupes de pixels seulement à moitié blancs. Plus l'image d'origine comporte de pixels ou plus on la regarde de loin, moins cette perte de qualité est visible à l'œil nu. La taille des images utilisées permet de s'adapter à l'âge et à la patience des élèves. Au lycée par exemple, il est possible de dessiner une image secrète sur une grille de taille 10x10. Cela peut sembler petit, mais il y a déjà 400 pixels à colorier sur la clé et l'image chiffrée. Une autre possibilité est de choisir une image secrète plus grande et de diviser le travail entre plusieurs élèves.

2.3 Variantes et adaptations

Une variante intéressante de la cryptographie visuelle implique l'utilisation d'images leurres : la clé secrète et l'image chiffrée ne sont 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.

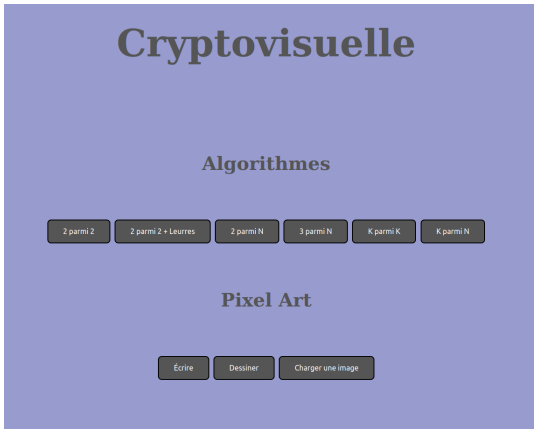


Pour cela, l'idée générale est qu'un pixel blanc de l'image secrète correspond à un bloc de quatre pixels dont 3 sont noirs sur les images superposées tandis qu'un pixel noir de l'image secrète correspond à un bloc de quatre pixels qui sont tous noirs. Un pixel blanc d'une image leurre correspond à un bloc de quatre pixels dont 2 sont noirs sur la clé ou l'image chiffrée, tandis qu'un pixel noir d'une image leurre correspond à un bloc de quatre pixels dont 3 sont noirs sur la clé ou l'image chiffrée. Pour chaque pixel de l'image secrète, il y a huit cas à considérer, selon la valeur de ce pixel et celle des pixels correspondants sur les images leurres. Cette variante est également réalisable en classe au lycée, mais peut-être décevante car les images devant apparaître sur la clé secrète et l'image bruitée sont très peu visibles, sauf à avoir un très grand nombre de pixels.

Une autre variante de la cryptographie visuelle permet de produire n images chiffrées, de telle sorte que seule la superposition d'au moins p images parmi les n images montre l'image secrète. Toutefois, les images générées sont alors très grandes, extrêmement fastidieuses à réaliser à la main et la perte de contraste est elle aussi très grande.

La cryptographie visuelle peut être étendue à des images plus complexes : différents niveaux de gris, différentes couleurs ou différents types de lumière. Plus l'image est complexe et plus on aura besoin de faire des traitements pour reconstruire l'image : on ne peut pas tout faire au crayon et à l'œil nu malheureusement !

Pour adapter l'activité à différents publics, le générateur en ligne [2] 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 différent formats et des gifs animés montrant le déchiffrement. Il permet aussi de générer des exemples pour les variantes avec les leurres et avec p images parmi n présentées ci-dessus.



Pour des lycéens à l'aise en Python, il est envisageable de coder les algorithmes de chiffrement, déchiffrement et 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.

3 Conclusion

Ces activités permettent d'illustrer le principe du chiffrement symétrique, où il faut avoir une clé secrète partagée entre deux personnes souhaitant communiquer, à travers la cryptographie visuelle.

Bibliographie

[1] Moni Naor and Adi Shamir. Visual cryptography. In Advances in Cryptology EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May9-12, 1994, Proceedings, volume 950 of Lecture Notes in Computer Science, pages 1–12. Springer, 1994.

[2] Site de génération des images chiffrées : https ://sancy.iut.uca.fr/ lafourcade/Cryptovisuelle