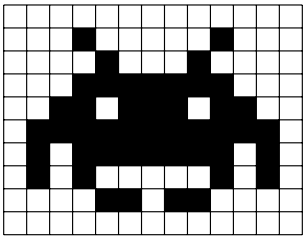
Mars 2015

Cryptographie visuelle

L'objectif de ce document est de présenter le fonctionnement de la cryptographie visuelle au travers d'exemples.

1 Introduction

La cryptographie visuelle a été inventée en 1994 par Moni Naor et Adi Shamir. 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 pixel 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*.



2 Fonctionnement 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.

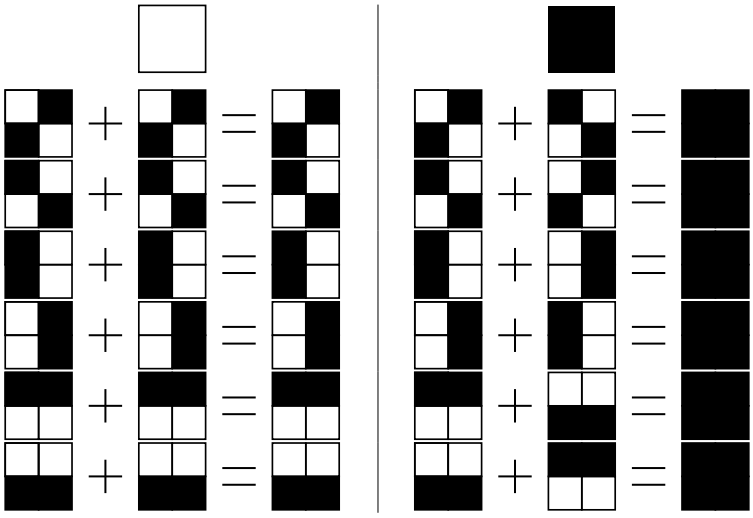
3 Construction du message secret

Partant d'une image en noir et blanc, il faut générer deux images telles qu'en les superposant elles révèlent le dessin original. Pour cela, chaque pixel de l'image de départ va devenir 4 pixels disposés en carré. Ainsi les deux images obtenues seront deux fois plus grandes, en nombre de pixel par ligne et par colonne, que l'image d'origine.

Un pixel blanc sur l'image de départ produit deux « images » de taille deux pixels par deux pixels en suivant les règles de gauche données ci-dessous. Pour chaque pixel blanc une règle est choisi aléatoirement parmi les 5 données ci-dessous.

Pour les pixels noirs, il faut prendre les règles de droite afin d'obtenir un carré de pixels tous noirs lors de la superposition. De même à chaque pixel noir il faut choisir aléatoirement une des 5 règles.

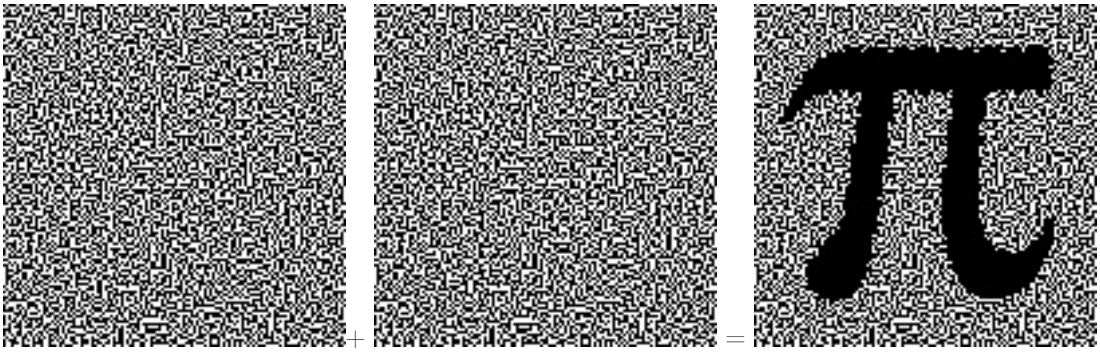
Ces règles ont pour objectif de donner deux images qui ont chacune autant de pixels noirs que de pixels blancs. Ainsi une image seule permet de ne retrouver aucune information sur l'image cachée, par contre lorsque les images seront superposées le dessin apparaîtra.



4 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 bloc blanc ne l'est plus. L'image finale ne sera pas exactement celle de départ. Elle sera moins « nette ».

5 Sécurité

Grâce à cette contruction, un attaquant qui observe un bloc de pixels n'est pas capable de savoir si la superposition permet d'obtenir un bloc blanc ou un bloc noir, car les règles de générations des images ont été choisies aléatoirement. Il faut les deux images pour pouvoir prédire si le pixel fusionné sera noir ou blanc.

6 Exercices

- Vous disposez d'un exemple sur la table qui, à partir de deux images, permet de reconstituer le symbole π.
- Vous disposez aussi d'un transparent d'image, de grilles de papier et de crayons. L'image est une grille de 14×14 pixels (soit 7×7 blocs).
  - *Comment remplir la grille pour faire apparaître un I au milieu de l'image superposée ?*
  - *Faut-il laisser des blancs ?*

7 Conclusion

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 !*