**Résumé détaillé et complet en français**

**Article :** *A new image encryption scheme based on a chaotic function*, Signal Porcessing : *Image Communication*

L’article, résumé ci-dessous, a été écrit dans l’optique de présenter une nouvelle méthode de chiffrement d’image simple et efficace. En effet, Internet a évolué et pouvoir garantir l’intégrité des images que l’on transmet ou stock par Internet est un vrai challenge, comme le disent les auteurs de l’article.

Il existe trois caractéristiques basiques de la cryptographie qui, une fois réunies, permettent d’avoir un système de chiffrement capable de résister à toute sorte d’attaques. Par exemple, des attaques de cryptanalyse ou par brute-force. La première de ces caractéristiques dit que pour toute clé utilisée, l’image chiffrée ne doit pas paraître différente du résultat d’une fonction aléatoire. Il s’agit d’une condition forte pour déduire d’un système son efficacité, on l’appelle l’*indiscernabilité.* Ensuite, vient la *confusion*, c’est-à-dire qu’il n’y a aucune ressemblance entre l’image en clair et l’image chiffrée. Enfin, la troisième caractéristique est la *diffusion*. Elle indique qu’une différence de un bit seulement dans la clé entraine des images chiffrées complètement différentes pour la même image en clair.

Pour que l’algorithme de chiffrement, présenté dans cet article, regroupent ces trois caractéristiques, les auteurs ont eu l’idée de lier plusieurs procédés mathématiques. Les systèmes chaotiques sont caractérisés par un phénomène appelé « sensibilité aux conditions initiales » (ici, la clé de chiffrement et l’image en clair). Ce phénomène, basé sur les congruences linéaires, donne une fonction qui utilise, ici, un modulo dégressif, afin d’obtenir une relation de récurrence. Cette fonction chaotique est couplée avec une opération XOR dans le processus de chiffrement pour rendre le système encore moins prédictible.

Cela nous amène aux conditions à remplir pour obtenir un tel système de chiffrement. En effet, pour assurer son efficacité, un tel système doit utiliser des clés assez larges dans son chiffrement (pour résister aux attaques brute-force), assurer le caractère aléatoire des images chiffrées (pour avoir une image chiffrée sécurisée qui ne peut pas être statistiquement distinguée d’une séquence véritablement aléatoire) et donc présenter une forte sensibilité aux conditions initiales (les valeurs utilisées pour la clé de chiffrement et l’image en clair).

L’algorithme de chiffrement réalisé à l’avantage d’être simple et de ne comporter que des entiers ;

La première chose à faire est de lire l’image I0, qui est une matrice N x M (longueur par largeur), et de stocker, dans l’ordre séquentiel, les valeurs de ses pixels en format binaire dans un tableau unidimensionnel, appelé vecteur Ib0. La taille L du tableau peut être calculée en fonction de la nature de l’image. Si il s’agit d’une image en niveaux de gris, sa taille sera L = 8 x N x M pour la valeur de gris du pixel qui donne 8 bits en binaire ; mais si il s’agit d’une image en couleur RGB, sa taille sera L = 3 x 8 x N x M pour les trois valeurs des couleurs Red, Green et Blue traduites en binaire.

La clé de chiffrement utilisée sera une suite de valeurs pseudo-aléatoires, comprises entre 1 et L, que l’on appellera g1,…,R et où R est le nombre de tours/boucles à faire pour obtenir une image chiffrée sécurisée ; Chaque boucle entraine de nouvelles permutations bit-à-bit.

R est donc le nombre de fois où l’on permute les bits de l’image. Il est issu du maximum entre R1, R2 et R3. Ces trois valeurs sont calculées de façon à avoir, parmi elles, un nombre de tours suffisant pour obtenir une image chiffrée efficace, résistante.

La deuxième étape consiste à permuter deux bits du tableau unidimensionnel initial grâce à la relation de récurrence : X= [[X \* Xmod S] \* X+ Xg] mod S ; où X = gr (la valeur g courante de la clé), Xg = X \* X et S = L-1 pour ne pas sortir du tableau. On transforme ensuite les éléments du vecteur Ib0 en Ib0[i] = Z3 et Ib0[j] = Z1 où i est la position courante dans le vecteur Ib0 et j est une nouvelle position chaotique j = i + 1 + Xi+1 avec la relation de récurrence, avec :

Z1 = Ib0[i],

Z2 = Ib0[j] = Ib0(I + 1 + Xi+1),

Z3 = Z1 ⊕ Z2, avec l’opération du OU Exclusif bit-à-bit, symbolisée par ⊕.

Cette étape est répétée jusqu’à avoir parcouru tout le tableau et on recommence tout pour un nouveau tour avec la valeur suivante de la clé gr.

La dernière étape regroupe simplement les bits du vecteur Ib0 par paquet de (3) x 8 pour reformer les pixels et donc l’image chiffrée IR.

L’algorithme de déchiffrement est le même que celui de chiffrement mais à l’envers. Cela signifie que l’on va prendre les valeurs de la clé dans l’ordre inverse de gR à g1. Les positions chaotiques j sont stockées dans un nouveau tableau unidimensionnel V. Ainsi, en parcourant V en partant de la fin, on récupère les valeurs de j dans le bon ordre pour permuter à nouveau les bits à leur emplacement initial.

Afin de s’assurer que cette méthode de chiffrement est correcte, il faut qu’elle respecte les trois caractéristiques de cryptographie décrites plus haut : *indiscernabilité, confusion, diffusion*. Pour cela, les auteurs ont réalisé plusieurs méthodes d’analyses et les ont présentées avec leurs résultats dans l’article.

Tout d’abord, parlons des trois méthodes présentées. Leur objectif est de valider la présence des trois caractéristiques précitées sur des images chiffrées grâce à l’algorithme présenté plus haut. Pour cela, ces méthodes vont être utilisées pour analyser la sensibilité du système de chiffrement à ses conditions initiales : la clé de chiffrement et l’image en clair, pour une image en couleurs RGB et une image en niveaux de gris à chaque analyse. Dans un premier temps, ces méthodes seront appliquées pour montrer la sensibilité à la clé de chiffrement.

La première méthode consiste simplement à analyser, dans un groupe d’images chiffrées provenant de la même image en clair, le caractère aléatoire de chacune des images chiffrées. Pour cela, l’analyse prend en compte les images chiffrées comme de simples séquences binaires qui passeront l’une après l’autre les tests statistiques de NIST (*National Institute of Standards and Technology of the U.S. Government*). Ils permettent d’évaluer le caractère aléatoire des séquences binaires. Seulement 1% d’échec est accepté. Les résultats obtenus montrent que les images chiffrées, provenant d’images en couleurs ou en niveaux de gris, ont toutes réussies les tests NIST et le ratio des séquences à avoir réussi le test est suffisamment élevé pour assurer de la qualité de ses images chiffrées selon la caractéristique de l’*indiscernabilité*.

La deuxième méthode analyse le niveau de corrélation entre les images chiffrées selon des calculs de coefficients de corrélation. Une absence de corrélation entre deux séquences obtient un coefficient nul. D’après les résultats présentés dans des histogrammes, les coefficients de corrélation sont négligeables ou nuls que ce soit pour les images en couleurs RGB ou en niveaux de gris. Ainsi, la qualité des images chiffrées concernant la caractéristique de *diffusion* est assurée. Des clés de chiffrement de un bit seulement de différent entraînent bien des images chiffrées différentes.

La troisième méthode concerne également le niveau de corrélation entre deux images chiffrée. Cependant, cette fois, elle utilise les indicateurs NPCR (*Number of Pixels Change Rate*) et UACI (*Unified Average Changing Intensity*), qui, respectivement, donne une évaluation en pourcentage des différences entre les valeurs des pixels de deux images, et mesure l’intensité moyenne des différences entre deux images. Ces calculs ont été effectués sur des images chiffrées avec des clés quasi-similaires. Or, les tableaux des résultats montrent que les images chiffrées sont très peu corrélées. Le système de chiffrement est donc très sensible à ses valeurs initiales (ici, les valeurs de la clé de chiffrement).

A présent, nous allons observer les résultats de ces méthodes mais, cette fois, pour montrer la sensibilité à l’image initiale : une différence de un bit dans l’image entraîne des images chiffrées complètement différentes (*diffusion*). On considère donc trois images presque identique (un bit de différence dans le même pixel) que l’on chiffre avec la même clé de chiffrement. Car comme nous l’avons vu précédemment, une clé de chiffrement différente de un bit entraîne déjà des images chiffrées différentes. Or, d’après les tableaux des résultats, les images chiffrées obtenues présentes encore une fois des corrélations négligeables entre elles. Même sur les analyses effectuées sur un plus gros échantillon d’images, les résultats restent stables. Le système de chiffrement est donc également très sensible à l’image en clair utilisée.

Le système de chiffrement basé sur une fonction chaotique couplée avec une opération XOR, proposé dans cet article, montre toutes les qualités d’un bon système de cryptographie, étant très sensible à ses conditions initiales : la clé de chiffrement et l’image en clair. Ce système a réussi toutes les analyses auxquelles il a été soumis. De plus, il n’utilise que des entiers et est simple à implémenter.

**Sources :**

<https://fr.wikipedia.org/wiki/Th%C3%A9orie_du_chaos>

*A new image encryption algorithm based on hyper-chaos*, de Tiegang Gao, Zengqiang Chen.

*Image encryption using chaotic logistic map*, de N.K. Pareek, Vinod Patidar K.K. Sud.

*A novel image encryption method based on total shuffling scheme*, de Guoji Zhang, Qing Liu.