Neuronal Crypto Système base sur la Carte Logistique

Naima Hadj-Said, Adda Ali-Pacha, Mohamed Sadek Ali-Pacha, Abdallah M'Hamed

Congrès francophone de doctorants en STIC MajecSTIC 2012 (MAnifestation des JEunes Chercheurs STIC)
du 29 au 31 novembre 2012 à l'université Lille, France,.

Neuronal Crypto Système basé sur la Carte Logistique

Naima HADJ-SAID[1] – Adda ALI-PACHA[1] – MS. ALI PACHA[1] – A. M'HAMED[2]
1.Université des Sciences et de la Technologie d'Oran USTO, BP 1505 El M'Naouer Oran 31036 ALGERIE tél./Fax : 213 – 041 / 46 26 85
E.Mail :nim_hadj@yahoo.fr
2.Institut National des Télécommunications Evry- Paris

Résumé: Les réseaux de neurones ont d'abord été développés pour résoudre des problèmes de contrôle, de reconnaissance de formes ou de mots, de décision, de mémorisation comme une alternative à l'intelligence artificielle.
On propose dans ce travail de les associer pour sécuriser les données multimédias stockées ou transmises, en utilisant les données de la carte logistique pour former les poids des synapses, de ce qu'on va appeler Neuronal Crypto-Système.

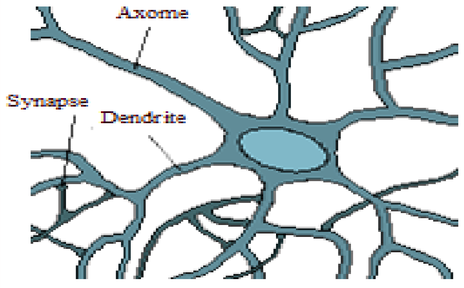
Cryptographie: La cryptographie est, historiquement, l'art de cacher une information pour la rendre inintelligible à toute personne ne connaissant pas un certain secret. Autrement dit, est l'ensemble des processus de verrouillage visant à protéger l'accès à certaines données afin de les rendre incompréhensible aux personnes non autorisées, autrement dit garantir la confidentialité, l'intégrité de ces informations, ainsi que leur imputabilité. Les algorithmes de chiffrement moderne utilisent la notion de clé notée K. Il existe deux classes de systèmes de cryptographie à base de clé :

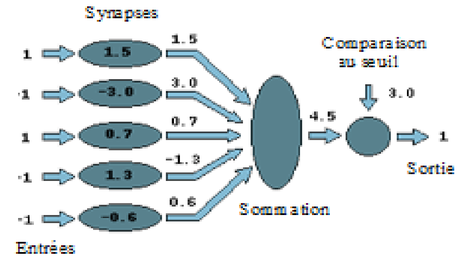
1. Les Systèmes à Clé Secrète : Permet de chiffrer et de déchiffrer des données à l'aide d'une clé unique.
2. Les Systèmes à Clé Publique : Propose un système mettant en scène deux clés. Celle qui permet l'encodage des données et une seconde clé destinée à décoder le contenu des messages. Le crypto système de Merkle-Hellman basé le problème du sac à dos (Knapsack Problem) est un exemple et qui est sous la forme suivante : Imaginons une collection de cailloux de poids $\{a_1, a_2, ... , a_n\}$ connus. Supposons que l'on place certains de ces cailloux dans un sac à dos et que l'on pèse le tout. Est-il possible, connaissant ce poids total, de savoir quels cailloux sont dans le sac ?

D'un autre côté, les réseaux de neurones artificiels sont des modèles informatiques de réseaux d'automates dont la structure et le comportement sont "copiés" sur ceux des neurones réels. À la façon du cerveau, ils peuvent reconnaître des formes, réorganiser des données et, de façon plus intéressante,

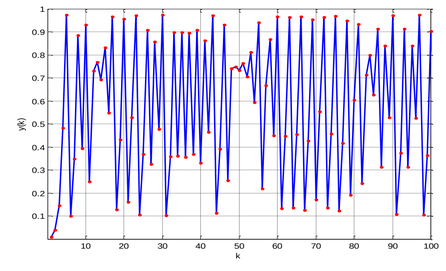
Réseaux de Neurones : L'idée principale des réseaux de neurones "modernes" est la suivante:
On se donne une unité simple, un neurone, qui est capable de réaliser quelques calculs élémentaires. On relie ensuite entre elles un nombre important de ces unités et on essaye de déterminer la puissance de calcul du réseau ainsi obtenu. Il est important de noter que ces neurones manipulent des données numériques et non pas symboliques.

Modèle Biologique d'une Cellule Neuronale: Dans le cerveau, les neurones sont reliés entre eux par l'intermédiaire d'axones et de dendrites. En première approche. On peut considérer que ces sortes de filaments sont conductrices d'électricité et peuvent ainsi véhiculer des messages depuis un neurone vers un autre. Les dendrites représentent les entrées du neurone et son axone sa sortie. Un neurone émet un signal en fonction des signaux qui lui proviennent des autres neurones. On observe en fait au niveau d'un neurone, une intégration des signaux reçus au cours du temps, c'est à dire une sorte de sommations des signaux. En général, quand la somme dépasse un certain seuil, le neurone émet à son tour un signal électrique.
La notion de synapse explique la transmission des signaux entre un axone et une dendrite. Au niveau de la jonction (c'est à dire de la synapse), il existe un espace vide à travers lequel le signal électrique ne peut pas se propager. La transmission se fait alors par l'intermédiaire de substances chimiques, les neuro-médiateurs. Quand un signal arrive au niveau de la synapse, il provoque l'émission de neuro-médiateurs qui vont se fixer sur des récepteurs de l'autre côté de l'espace inter-synaptique. Quand suffisamment de molécules se sont fixées, un signal électrique est émis de l'autre côté et on a donc une transmission. En fait, suivant le type de la synapse, l'activité d'un neurone peut renforcer ou diminuer l'activité de ces voisins. On parle ainsi de synapse excitatrice ou inhibitrice.





Théorie du Chaos :
Le "chaos" est le terme utilisé pour décrire le comportement apparemment complexe de ce que nous considérons être simples. Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non linéaire. Du point de vue mathématique la notion générale de système dynamique est défini à son tour à partir d'un ensemble de variables qui forment le vecteur d'état dans notre cas, c'est la carte logistique est l'une des dynamiques très connues dans la théorie des systèmes non-linéaires et qui définit par l'équation suivante :$y_{k+1} = r.\ x_k.(1 - x_k)$, Pour une condition initial $x_0 = 0.01$ et $r = 3.9$ on obtient le graphe suivant.



Neuronal Crypto-Système

- On prend un crypto-système inspiré de la figure 2 où : Les entrées $\{M_i,\ i \geq 1...\}$ sont les caractères du texte en clair.
- Synapses $\{W_i,\ i \geq 1\ldots\}$ sont des valeurs réelles positives issues de la carte logistique.
- Sommation $C = \sum W_i M_i$ et la sortie la valeur numérique de C selon la norme IEEE 754.

Chiffrement du Neuronal Crypto-Système

- Le texte en clair est chiffré caractère par caractère (le caractère de 8 bits).
- Faire dérouler un programme d'un système chaotique dans notre cas c'est la carte logistique et avec les valeurs initiales prédéfinies.
- On prend les valeurs supérieures aux valeurs initiales et chaque fois un paquet de huit valeurs, qu'on va les traitées, c'est-à-dire on va ordonner leur valeurs absolues de façon décroissante et puis on norme ces derniers par rapport à leur plus grande valeur.
- On calcul les synapses de la façon suivante :
- La 1ère synapse prend la grande valeur traitée.
- La 2ème synapse prend la somme deux grandes valeurs traitées.
- La 3ème synapse prend la somme des trois grandes valeurs traitées, et ainsi de suite jusqu'à la 8ème synapse prend la somme de toutes les valeurs traitées.
- On aura la valeur 1ère synapse est inférieure strictement à la valeur 2ème synapse qui est inférieure strictement à la valeur 3ème synapse et ainsi de suite…
- On associé à la 8ème synapse le 1er bit à gauche du texte en clair, le 2ème bit de ce texte on lui associé la 7ème synapse, ainsi de suite jusqu'au 8ème bit on lui associé la 1ère synapse.
- La sommation est effectuée selon la valeur des bits du caractère du texte en clair, multipliée par les valeurs des synapses qui leur sont associées.
- La valeur de cette somme est écrite sous forme numérique selon la norme IEEE 754 simple précision, mais on ne prend que (4 bits pour l'exposant et 12 bits pour la mantisse) un nombre de 16 bits, donc le caractère chiffré est représenté sur deux caractères.
- On passe au chiffrement d'un autre caractère en suivant les mêmes démarches.

Conclusion : A partir d'un modèle simple des neurones artificiels on a construit un système cryptographique. On sait que les connexions entre les neurones composant le réseau décrivent la topologie du modèle. Elle peut être quelconque, mais le plus souvent il est possible de distinguer une certaine régularité (réseau à connexion complète).
Dans notre modèle nous avons utilisé la structure d'un réseau monocouche est telle que des neurones organisés en entrée soient entièrement connectés à d'autres neurones organisés en sortie par une couche modifiable de poids par la sélection des valeurs aléatoires issus de la carte logistique dans notre cas.