République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي و البحث العلمي

Mémoire de fin d'études

Pour l'obtention du diplôme d'Ingénieur d'État et Master 2 en Informatique

Option : ingénierie des systèmes informatiques

An efficient and robust image encryption scheme tailored for modern applications requirements

Réalisé par :
M. Khebchi Abdallah

Encadré par :
Dr. Amina Souyah
(ESI-SBA)

Soutenu le 29 juin 2022, Devant le jury composé de :

Dr. Djihed Anani (Président) : ESI-SBA
Dr. Miloud Khaldi (Examinatur) : ESI-SBA

Promotion : 2021/2022

Abstract

Data security is a crucial aspect that is required especially when dealing with open-networks, in order to withstand to security attacks that are constantly on rise leading to drastic consequences. Several security services are highly needed, aiming to prevent both passive and active attacks such as Data Confidentiality (DC). A DC service is typically ensured by means of symmetric cipher algorithms. However, traditional encryption algorithms such as Data Encryption Algorithm (DES), Advanced Encryption Standard (AES),...,etc., are not the adequate means to deal with digital images' features (e.g., large data size, high redundancy, strong pixel correlation,..., etc.) since they are addressed to preserve textual data content. Moreover, these traditional algorithms employ a static structure (i.e., substitution and diffusion primitives are fixed and not depending to the secret key) leading to multi-round encryption routine to achieve satisfactory level of security. To this end, there is an urgent need to design new symmetric cipher algorithms that can deal well with digital images' features and that can take a good balance between sufficient security degrees and time performance.
Keeping in view the importance of designing new symmetric cipher algorithms for image content preservation, this thesis is concerned by image data confidentiality preservation, for which symmetric cipher algorithm with dynamic encryption structure is handled, for the sake of decreasing the employed number of rounds (only two rounds). Literature review has been carried out by incorporating recent key papers related to image encryption, from which we selected the research contribution (Fawaz et al. 2016) to redesign and realize by adjusting the dynamic key to be both secret key and plain image related, rendering the scheme output highly connected to both of its inputs, namely secret key and plain image, aiming to elevate both the diffusion mechanism and the avalanche effect. Moreover , we added the image authentication using HMAC along with SHA-512 hashing algorithm to insure the image integrity between the sender and receiver .
A number of series experiments have been carried out to evaluate the effectiveness of our contribution, the obtained results validated the robustness of the our scheme against all the considered types of attacks.

Keywords : Data security, cryptography, Data Confidentiality (DC), image encryption, dynamic encryption structure.

Résumé

La sécurité des données est un aspect crucial qui est nécessaire en particulier lorsqu'il s'agit de réseaux ouverts, afin de résister aux attaques de sécurité qui ne cessent d'augmenter, entraînant des conséquences dramatiques. Plusieurs sécurité les services sont très nécessaires, visant à prévenir les attaques passives et actives telles que la confidentialité des données (DC). Un service DC est typiquement assuré au moyen d'algorithmes de chiffrement symétriques. Cependant, traditionnelle algorithmes de chiffrement tels que Data Encryption Algorithm (DES), Advanced Encryption Standard (AES),..., etc., ne sont pas les moyens adéquats pour traiter les caractéristiques des images numériques (par exemple, grande taille de données, haute redondance, forte corrélation de pixels,..., etc.) puisqu'ils sont adressés pour préserver le contenu des données textuelles. De plus, ces algorithmes traditionnels utilisent une structure statique (c'est-à-dire des primitives de substitution et de diffusion sont fixes et ne dépendent pas de la clé secrète) conduisant à une routine de chiffrement à plusieurs tours pour atteindre niveau de sécurité satisfaisant. A cette fin, il est urgent de concevoir un nouveau chiffrement symétrique algorithmes qui peuvent bien gérer les caractéristiques des images numériques et qui peuvent prendre un bon équilibre entre degrés de sécurité suffisants et performances temporelles .
Gardant à l'esprit l'importance de concevoir de nouveaux algorithmes de chiffrement symétriques pour le contenu des images conservation, cette thèse s'intéresse à la préservation de la confidentialité des données d'images, pour laquelle l'algorithme de chiffrement avec structure de chiffrement dynamique est géré, dans le but de réduire le temps utilisé nombre de tours (seulement deux tours). Une revue de la littérature a été effectuée en incorporant les clés récentes articles liés au chiffrement d'images, parmi lesquels nous avons sélectionné la contribution de la recherche (Fawaz et al. 2016) à reconcevoir et réaliser en ajustant la clé dynamique pour qu'elle soit à la fois secrète liés à la clé et à l'image simple, rendant la sortie du schéma hautement connectée à ses deux entrées, à savoir clé secrète et image simple, visant à élever à la fois le mécanisme de diffusion et l'effet d'avalanche . De plus, nous avons ajouté l'authentification d'image utilisant HMAC avec l'algorithme de hachage SHA-512 pour assurer l'intégrité de l'image entre l'expéditeur et le destinataire. Un certain nombre d'expériences en série ont été menées pour évaluer l'efficacité de notre contribution, les résultats obtenus ont validé la robustesse de notre schéma contre tous les types d'attaques considérés.

Mots clés : Sécurité des données, cryptographie, Confidentialité des données (DC), chiffrement d'images, structure de chiffrement dynamique.
