European Journal of Computer Science and Information Technology
Vol.11, No.1, pp.1-8, 2023
Print ISSN: 2054-0957 (Print),
Online ISSN: 2054-0965 (Online)

Chiffrement et déchiffrement d'images à l'aide de l'algorithme AES

Elisée Ilunga Mbuyamba, Simon Tshibengabu Kalonji
Institut Supérieur de Techniques Appliquées
Kinshasa, RD Congo

DOI : https://doi.org/10.37745/ejcsit.2013/vol11n118 Published : 18th January 2023

Citation : Mbuyamba E.I. and Kalonji S.T (2023) Chiffrement et déchiffrement d'images à l'aide de l'algorithme AES, *European Journal of Computer Science and Information Technology*, Vol.11, No.1, pp.1-8

RESUME : *Dans cet article nous allons parler du chiffrement et déchiffrement d'images en utilisant l'algorithme AES. Ce type de cryptage est appelé symétrique car il utilise une même clé pour chiffrer et déchiffrer l'information. L'algorithme AES (Advanced Encryption Standard) est le plus utilisé dans le chiffrement symétrique à cause de sa robustesse due à la clé de 256 bits qui est difficile à casser. Nous avons choisi de manière aléatoire des images dans l'ensemble des données ILSVRC2012 pour illustrer le fonctionnement du cryptage symétrique avec l'algorithme AES. Ces images ont été premièrement chiffrées et ensuite déchiffrées à l'aide d'une même clé. Les résultats obtenus nous ont démontré que l'image cryptée permettait de garantir la confidentialité de l'information. Nous avons également fait recours à des métriques d'évaluation de qualité d'images pour vérifier que la qualité de l'image décryptée restait égale à celle de l'originale.*
MOTS CLES : Cryptage symétrique, AES, confidentialité

ABSTRACT: *In this paper we will talk about encryption and decryption of images using the AES algorithm. This type of encryption is called symmetric because it uses the same key to encrypt and decrypt information. The AES (Advanced Encryption Standard) algorithm is the most used in symmetric encryption because of its robustness due to the 256-bit key which is difficult to break. We randomly chose images from the ILSVRC2012 dataset to illustrate how symmetric encryption works with the AES algorithm. These images were first encrypted and then decrypted using the same key. The results obtained showed us that the encrypted image made it possible to guarantee the confidentiality of the information. We also used image quality evaluation metrics to verify that the quality of the decrypted image remained equal to that of the original.*

KEYWORDS: Symmetric encryption, AES, confidentiality

INTRODUCTION

La sécurité d'information est devenue l'un des problèmes de grande préoccupation dans notre société. Le NIST (National Institute of Standards and Technology) dans son Computer Security Handbook [1] définit le terme sécurité informatique comme étant la protection d'un système d'information automatisé afin d'atteindre les objectifs applicables de préservation de l'intégrité, la disponibilité et la confidentialité des ressources du système d'information (y compris le matériel, les logiciels, les micrologiciels, les informations/données et les télécommunications).
Cette définition introduit trois objectifs clés qui sont au centre de la sécurité informatique, à savoir :

1. **Confidentialité** (Confidentiality) :
La confidentialité des données garantit que les informations privées ou confidentielles ne sont pas mises à la disposition ou divulguées à des personnes non autorisées.
2. **Intégrité** (Integrity) :
— Intégrité des données : garantit que les informations et les programmes ne sont modifiés que d'une manière spécifiée et autorisée.
— Intégrité du système : assure qu'un système exécute sa fonction prévue de manière intacte, sans manipulation non autorisée délibérée ou par inadvertance du système.
3. **Disponibilité** (Availability) :
La disponibilité des systèmes garantit qu'ils fonctionnent rapidement et que le service n'est pas refusé aux utilisateurs autorisés à tout moment.

Par ailleurs, il faut garantir la non-répudiation et l'authenticité des informations. Nous entendons par non-répudiation le fait que l'émetteur d'un message ne puisse nier l'avoir envoyé et le récepteur l'avoir reçu. Et par authentification le fait de s'assurer de l'identité d'un objet, généralement une personne, mais parfois un serveur, une application.

L'approche principale pour sécuriser l'information stockée et transmise contre les individus indésirables est de la convertir en une forme non reconnaissable par ses attaquants, et ceci est connu sous le nom de cryptographie [2]. Elle permet de chiffrer les données (pour les stocker ou les transmettre) et ensuite les déchiffrer lorsqu'on a besoin de l'information originale. Le système qui offre ces deux fonctions, c.-à-d., chiffrement et déchiffrement est appelé cryptosystème. Il existe deux grandes familles d'algorithmes utilisés dans les cryptosystèmes incluant : les algorithmes de chiffrement symétriques et les algorithmes de chiffrement asymétriques (à clé publique). Dans le premier groupe nous retrouvons des techniques telles que DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard), etc. Et dans le second nous avons des algorithmes tels que RSA (Rivest–Shamir–Adleman), Échange de clés Diffie-Hellman, DSS (Digital Signature Standards), ECC : Elliptic Curve Cryptography, etc.

De nos jours, la multiplicité des réseaux sociaux, d'application web et d'objets connectés à internet permet d'engendrer un volume important de trafic des données multimédias sur internet. De ce fait, la sécurité des données a attiré beaucoup des groupes de recherche ces dernières années. Dans [3], les auteurs présentent un algorithme basé sur AES modifié pour le chiffrement d'images. Une nouvelle conception basée sur des clés chaotiques pour le cryptage et le décryptage d'images a été proposé dans [4]. Dans le même ordre d'idée, les auteurs de [5, 6] présentent un chiffrement et un déchiffrement d'images utilisant l'algorithme AES.

Dans cet article, nous présentons l'application de l'algorithme AES dans le chiffrement et déchiffrement des images. L'algorithme AES a remplacé le DES en offrant plus de sécurité. Ce travail est organisé de la manière suivante : Dans la Section 2, les principes de base du chiffrement et déchiffrement sont présentés. Les résultats de l'application du chiffrement et déchiffrement grâce à l'algorithme AES sont présentés dans la Section 3. Enfin, la conclusion de cet article sera faite dans Section 4.

METHODE

La technique universelle pour assurer la confidentialité des données transmises ou stockées est le chiffrement symétrique. Nous allons nous focaliser sur l'AES, qui est un algorithme de chiffrement par blocs.

A. Structure de chiffrement symétrique

Le cryptage symétrique, également appelé cryptage conventionnel ou cryptage à clé unique, était le seul type de cryptage utilisé avant l'introduction du cryptage à clé publique à la fin des années 1970. Son principe de fonctionnement de base est décrit dans la Figure 1. Il reste le plus largement utilisé des deux types de cryptage.

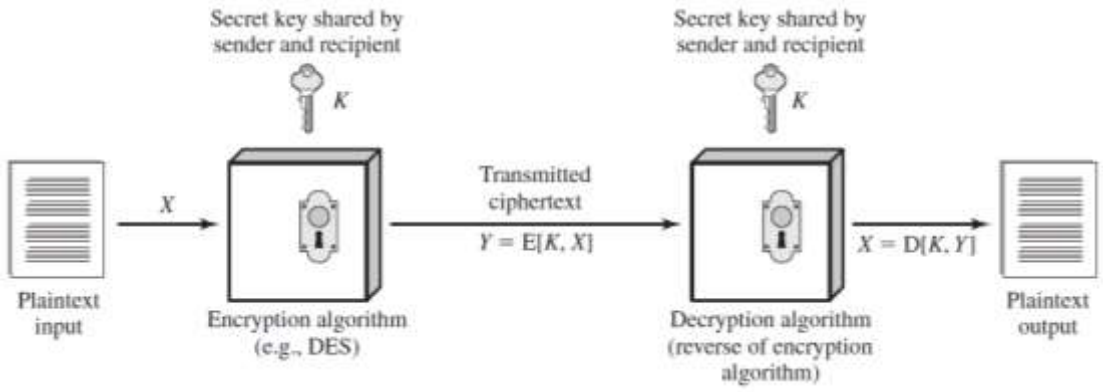


Figure 1. Principe du chiffrement symétrique, voir [7]

Le chiffrement est effectué conformément à la formule ci-après :

$$Y = E[K, X]$$

Et le déchiffrement par :

$$X = D[K, Y]$$

Où

• X représente le texte en clair (Plaintext) : il s'agit du message ou des données d'origine qui sont introduits dans l'algorithme en tant qu'entrée.
• E désigne l'algorithme de chiffrement (Encryption algorithm) : L'algorithme de chiffrement effectue diverses substitutions et transformations sur le texte en clair.
• K est la clé secrète (secret key) : La clé secrète est également entrée dans l'algorithme de cryptage. Les substitutions et transformations exactes effectuées par l'algorithme dépendent de la clé.
• Y correspond au texte chiffré (Ciphertext) : Il s'agit du message brouillé produit en sortie. Cela dépend du texte en clair et de la clé secrète. Pour un message donné, deux clés différentes produiront deux textes chiffrés différents.
• D désigne l'algorithme de décryptage (Decryption algorithm) : il s'agit essentiellement de l'algorithme de cryptage exécuté à l'envers. Il prend le texte chiffré et la clé secrète et produit l'original texte en clair.

Algorithmes de chiffrement par blocs symétriques
Les algorithmes de chiffrement symétrique les plus couramment utilisés sont les chiffrements par blocs. Ils traitent l'entrée de texte en clair dans des blocs de taille fixe et produit un bloc de texte chiffré de taille égale pour chaque bloc de texte en clair. L'algorithme traite des quantités de texte en clair plus longues sous la forme d'une série de blocs de taille fixe. Les algorithmes symétriques les plus importants, qui sont tous des chiffrements par blocs, sont le Data Encryption Standard (DES), le triple DES et le Advanced Encryption Standard (AES).

	DES	**Tripe DES**	**AES**
Taille de bloc de texte en clair (bits)	64	64	128
Taille de bloc de texte chiffré (bits)	64	64	128
Taille de la clé (bits)	56	112 ou 168	128, 192, ou 256

Le niveau de sécurité d'un algorithme de chiffrement est mesuré par la taille de sa clé. Plus la taille de la clé est grande, plus l'attaquant a besoin de temps pour effectuer la recherche exhaustive de la clé. Par conséquent, le niveau de sécurité devient aussi élevé. Nous pouvons déjà constater que l'AES est l'algorithme qui nous offrira plus de sécurité grâce à sa taille de clé de 256, qui fournirait $2^{256} \approx 1.2 \times 10^{77}$ possible clés à chercher.

En cryptographie, un mode d'opération est la manière de traiter les blocs de texte clairs et les chiffrés au sein d'un algorithme de chiffrement par bloc. Plusieurs modes existent, nous citerons:

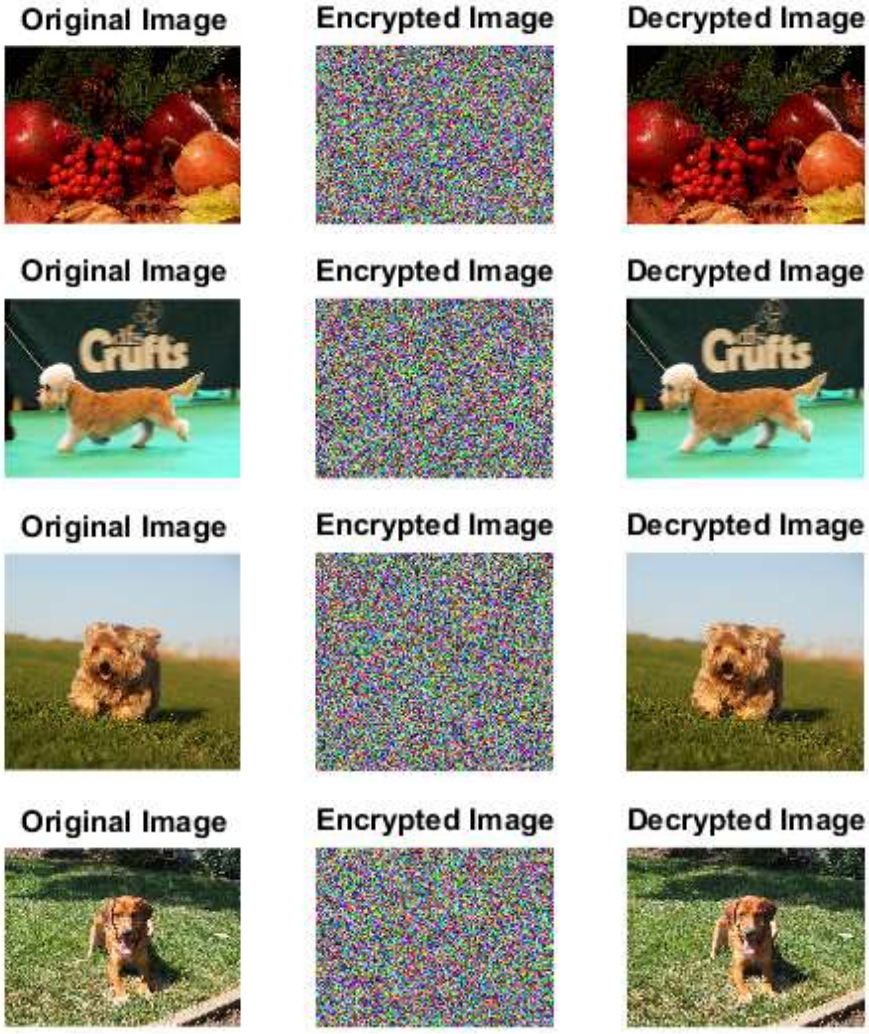
- Dictionnaire de codes (Electronic Code Book, ECB)
- Enchaînement des blocs (Cipher Block Chaining, CBC)
- Chiffrement à rétroaction (Cipher Feedback, CFB)
- Chiffrement à rétroaction de sortie (Output Feedback, OFB)
- Chiffrement basé sur un compteur (CounTeR, CTR)

- Chiffrement avec vol de texte (CipherText Stealing, CTS)
- Compteur avec CBC-MAC
- EAX (inventé par David Wagner et al.)
- CWC (à deux passes)

Dans le chiffrement symétrique l'algorithme opère sur un bloc de 64 ou 128 bits à ce jour. Les messages électroniques, les paquets réseau, les enregistrements de base de données et d'autres sources de texte en clair doivent être divisés en une série de blocs de longueur fixe pour le chiffrement par bloc symétrique.

RESULTATS

Dans cette Section, nous allons présenter et discuter sur les résultats obtenus en utilisant l'algorithme AES pour chiffrer et déchiffrer les images. Les images utilisées pour nos tests ont été extraites de l'ensemble des données (dataset) ILSVRC2012 [8]. Les Figure 2 et 3 illustrent comment des images sont premièrement chiffrées à l'aide de l'algorithme AES, et ensuite déchiffrées pour retrouver les images originales.



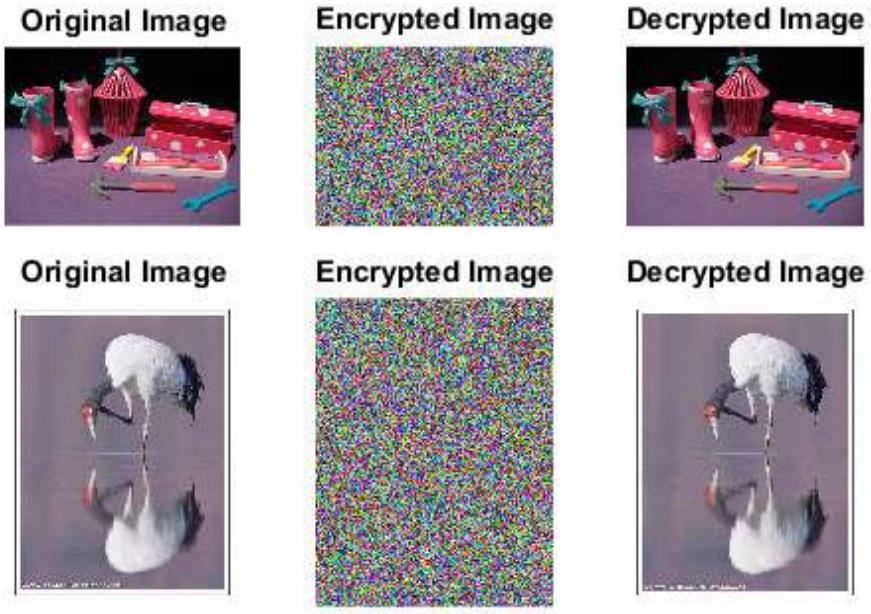
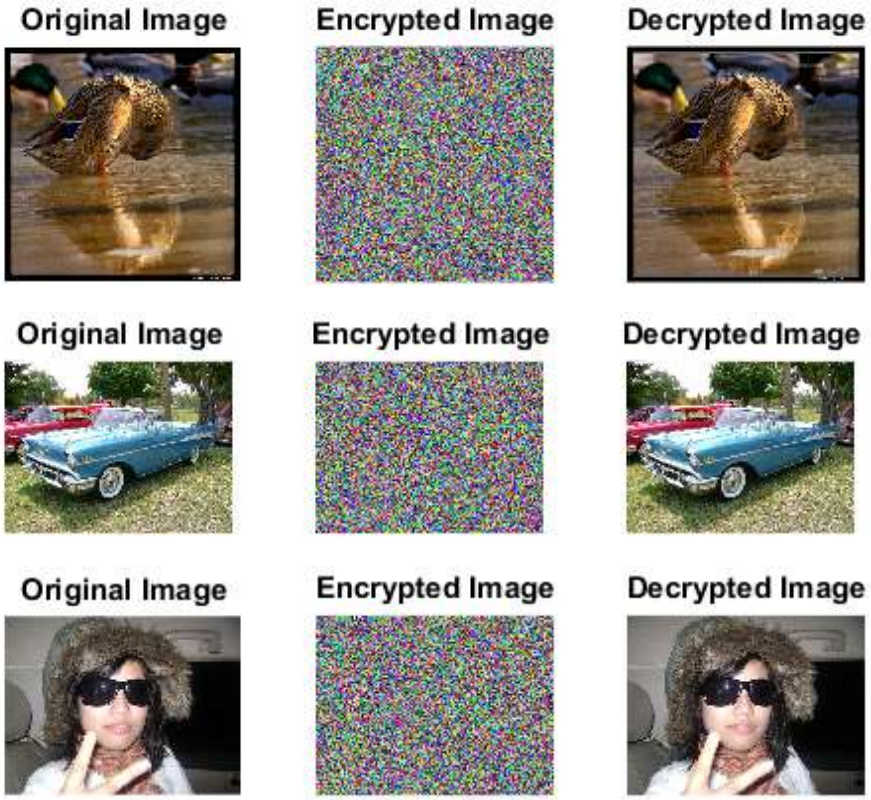


Figure 2. Résultat du chiffrement et déchiffrement avec l'AES



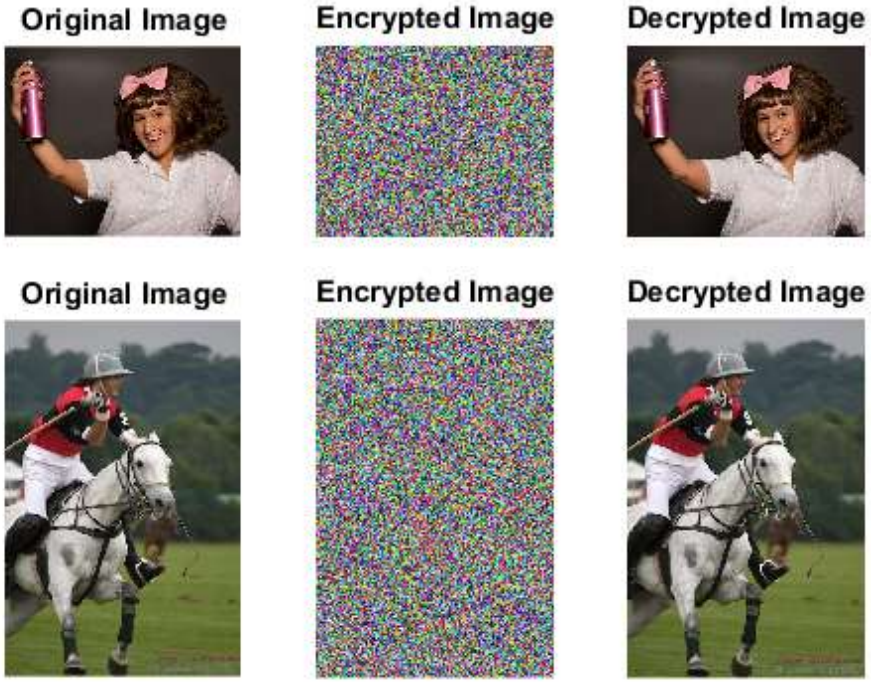


Figure 3. Résultat du chiffrement et déchiffrement avec l'AES

Pour vérifier que la qualité de l'image déchiffrée par rapport à l'originale n'a pas été entamée par l'opération de chiffrement, il est recommandé d'utiliser certaines métriques d'évaluation de qualité d'image telles que le PSNR (Peak Signal to Noise Ratio), EQM (Erreur Quadratique Moyenne) connue sous le nom MSE (Mean Squared Error) en anglais.
Le PSNR est défini par la formule suivante :

$$PSNR = 10\ log_{10}(\frac{d^2}{MSE})$$

Où d est la dynamique du signal (la valeur maximum possible pour un pixel), dans le cas standard d'une image codée sur 8-bits, d=255.
L'Erreur Quadratique Moyenne est définie pour 2 images I_o et I_r de taille $M \times N$ par la formule suivante :

$$MSE = \frac{1}{MN}\sum_{i-0}^{M-1}\sum_{j-0}^{N-1}(I_o(i,j) - I_r(i,j))^2$$

Le calcul de ces deux métrique pour toutes les images a donné infinie pour le PSNR et zéro pour le MSE. Ce qui signifie que la qualité de l'image reconstruite I_r (image déchiffrée) est égale à celle de l'origine I_o.

CONCLUSION

Dans cet article nous avons présenté le cryptage symétrique à l'aide de l'algorithme AES. Nous avons appliqué cet algorithme sur des images sélectionnées de manière aléatoire dans l'ensemble des données ILSVRC2012. Les résultats nous ont montré que les images cryptées permettaient de rendre inaccessible l'information qu'elles contenaient. Cette observation était satisfaisante car elle garantissait la confidentialité de l'information, un des objectifs clé de la sécurité des données. Par ailleurs, il a été aussi vérifié que les images décryptées étaient totalement similaire à l'originale.

References

[1] National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12, October 1995.
[2] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology (WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.
[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", 2007.
[4] Jui-Cheng Yen and Jim-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", 2000.
[5] Roshni Padate, Aamna Patel, "Image Encryption And Decryption Using AES Algorithm", 2014.
[6] P. Radhadevi, P. Kalpana, "Secure Image Encryption Using Aes",2012.
[7] William Stallings, Lawrie Brown, Computer Security – Principles and Practice (Third Edition), Pearson Education, 2015
[8] Olga Russakovsky and Jia Deng and Hao Su and Jonathan Krause and Sanjeev Satheesh and Sean Ma and Zhiheng Huang and Andrej Karpathy and Aditya Khosla and Michael Bernstein and Alexander C. Berg and Li Fei-Fei, ImageNet Large Scale Visual Recognition Challenge, International Journal of Computer Vision (IJCV), Vol 115, 2015