**La généralisation rapide des communications par Internet a engendré une croissance rapide de transmission des informations multimédia telles que les images (IRM, Scanner X, médecine nucléaire, etc.), cette transmission se fait à travers des réseaux indiscrets et ouverts ce qui entraîne une augmentation des fraudes par vol d'informations des patients, en raison d'un manque de sécurité sur ces liens. Or, les documents médicaux d'un individu représentent des informations confidentielles qui exigent des protocoles et une sécurité stricte, principalement pour protéger l'identité de l’individu qui ne devrait être accessible que par leur personnel autorisé [1]. Par conséquent, chaque fois qu'une image numérique doit être utilisée dans une application, la préservation de son contenu devient un problème critique.**

**Dans ces conditions des nouvelles méthodes ont été développées, il s’agit de méthodes de cryptage cette solution qui trouve ses origines en Rome antique, avec le tout premier code de chiffrement connu, le code de César. Ce chiffrement consiste à remplacer chaque lettre d’un message par une lettre plus loin dans l’alphabet dans ces premières utilisations la cryptographie est basée, donc, sur un « simple » algorithme de substitution de caractères, Au fil des siècles les chercheurs n’ont cessé de développer des nouvelles méthodes de cryptage comme DES, IDEA ou AES [2]. Mais ces méthodes traditionnelles ne sont pas adéquates pour traiter les exigences de contenu de données visuelles, en raison des caractéristiques spécifiques des images numériques telles que la grande taille des données, la forte corrélation des pixels et la redondance élevée, et car elles sont à l'origine conçues pour sécuriser les données textuelles**. De plus, ces moyens traditionnels semblent ne pas être efficaces, en particulier pour une utilisation pratique en ce qui concerne la vitesse et la puissance non raisonnables du matériel pour effectuer un cryptage d'image. D'autre part, en raison de l'augmentation de quantité de données échangées via les systèmes de communications ; L'un des problèmes émergents est qu'une taille croissante des images , en particulier des images fixes, est inévitable en raison du besoin d'images de haute qualité qui est requise énormément dans le domaine médical. En conséquence, un besoin d'espaces de stockage plus importants suit. Bien que les techniques de stockage sur les ordinateurs numériques aient connu un développement rapide, elles nécessitent souvent la réduction du stockage des données numériques. L'une de ces réductions par se tourner vers les formats compressés (JPEG). Face à ces deux problèmes ; compression des images et assurer leur sécurité, la question qui se pose, pourquoi ne pas avoir les deux en même temps ; compression et chiffrement sachant que la réalisation de ces deux concepts en cascade induit un certain nombre de défis. En effet, la compression des données et leur cryptage ultérieur ou inversement peuvent réduire le taux de compression ainsi que la robustesse de cryptage. Pour résoudre ce problème, plusieurs approches combinées ont été proposées, cependant ces méthodes entraînent généralement des problèmes de sécurité ou d’efficacité de la compression dans la pratique. Certains d’eux souffre d’une réduction substantielle de l’efficacité de la compression en raison de la réduction de la corrélation entre les pixels des images causés par les opérations de cryptage d’autre sont mois résistants devant les attaques de texte en claire ou contiennent des failles de sécurité.

Je propose dans mon étude une nouvelle méthode de cryptage d’image qui a été proposée basée sur la matrice House Holder, pour éliminer la complexité de calculé l’inverse de la clé de déchiffrement, ainsi, facilite la transmission de cette clé. Aussi, elle utilise une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion, pour chiffrer les images qui contiennent des grandes zones d'une couleur unique [3], Enfin, nous allons montrer l’efficacité et la sécurité de notre méthode proposé, Donc en utilisant différentes mesures d’évaluation pour montrer la sécurité et l’efficacité de l’algorithme proposé. Nous allons présenter les plus important comme : tests statistique tel que (l’histogramme, la corrélation, l’entropie) et les tests différentiels tel que (UACI, NPCR), l’espace de clés, la sensibilité de la clé. Tout cela on le projetant dans le langage Python.

La préservation de son contenu devient un problème critique. En raison des caractéristiques spécifiques des images numériques telles que la grande taille des données, la forte corrélation des pixels et la redondance élevée, les méthodes de cryptage traditionnelles telles que DES, IDEA ou AES, ne sont pas adéquates pour traiter les exigences de contenu de données visuelles, car elles sont à l'origine conçues pour sécuriser les données textuelles. De plus, ces moyens traditionnels semblent ne pas être efficaces, en particulier pour une utilisation pratique en ce qui concerne la vitesse et la puissance non raisonnables du matériel pour effectuer un cryptage d'image

**La généralisation rapide des communications par Internet a engendré une croissance rapide de transmission des informations multimédia telles que les images (IRM, Scanner X, médecine nucléaire, etc.), cette transmission se fait à travers des réseaux indiscrets et ouverts ce qui entraîne une augmentation des fraudes par vol d'informations des patients, en raison d'un manque de sécurité sur ces liens. Or, les documents médicaux d'un individu représentent des informations confidentielles qui exigent des protocoles et une sécurité stricte, principalement pour protéger l'identité de l’individu qui ne devrait être accessible que par leur personnel autorisé [1]. Par conséquent, chaque fois qu'une image numérique doit être utilisée dans une application, la préservation de son contenu devient un problème critique.**

**Dans ces conditions des nouvelles méthodes ont été développées, il s’agit de méthodes de cryptage cette solution qui trouve ses origines en Rome antique, avec le tout premier code de chiffrement connu, le code de César. Ce chiffrement consiste à remplacer chaque lettre d’un message par une lettre plus loin dans l’alphabet dans ces premières utilisations la cryptographie est basée, donc, sur un « simple » algorithme de substitution de caractères, Au fil des siècles les chercheurs n’ont cessé de développer des nouvelles méthodes de cryptage comme DES, IDEA ou AES [2]. Mais ces méthodes traditionnelles ne sont pas adéquates pour traiter les exigences de contenu de données visuelles, en raison des caractéristiques spécifiques des images numériques telles que la grande taille des données, la forte corrélation des pixels et la redondance élevée, et car elles sont à l'origine conçues pour sécuriser les données textuelles**. De plus, ces moyens traditionnels semblent ne pas être efficaces, en particulier pour une utilisation pratique en ce qui concerne la vitesse et la puissance non raisonnables du matériel pour effectuer un cryptage d'image. D'autre part, afin d'établir un diagnostic à distance. De plus, l'appareil d'acquisition d'images médicales peut se trouver dans une ambulance ou dans tout autre véhicule mobile, et dans ce cas la transmission est effectuée par l'intermédiaire de réseaux sans fil. Pour des raisons vitales, dans ce type d'applications, les images doivent être transmises rapidement et sûrement, Face à ces problèmes, plusieurs approches combinées ont été proposées, cependant ces méthodes entraînent généralement des problèmes de transmission de la clé de déchiffrement ce qui engendre un manque de rapidité dans la pratique. Certains d’eux sont vulnérable aux attaques ; telles que les attaques en texte clair choisies ou connues par exemple e chiffrement de Hill, le chiffre de Vigenère et le chiffre d’Affine.

Je propose dans mon étude une nouvelle méthode de cryptage d’image qui a été proposée basée sur la matrice House Holder, pour éliminer la complexité de calculé l’inverse de la clé de déchiffrement, ainsi, facilite la transmission de cette clé. Aussi, elle utilise une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion, pour chiffrer les images qui contiennent des grandes zones d'une couleur unique [3], Enfin, nous allons montrer l’efficacité et la sécurité de notre méthode proposé, Donc en utilisant différentes mesures d’évaluation pour montrer la sécurité et l’efficacité de l’algorithme proposé. Nous allons présenter les plus important comme : tests statistique (l’histogramme, la corrélation, l’entropie) et les tests différentiels (UACI, NPCR), l’espace de clés, la sensibilité de la clé. Tout cela on les projetant dans l’espace Python.

Notre travail est de présenter l’approche de cryptage pour contribuer a` augmenter la s´écurie du partage en permettant de garder la confidentialité des données du patient et de vérifier l’intégrité et l’authenticité des images médicales à la fois

La cryptographie est parmi les méthodes les plus efficaces pour établir la confidentialité et l’intégrité de ce type d’information qui sont considérées comme des données particulières en raison de leurs tailles et de leurs informations qui sont de natures bidimensionnelles et redondantes [2].

Ces particularités des données rendent les algorithmes développés dans la littérature inutilisables sous leurs formes classiques, à cause des contraintes de la vitesse et de la perte de l’information qui peuvent être causées par un crypto système classique tel que le chiffrement de Hill qu’il s’agit d’un code simple à appréhender ou le chiffrement affine qui est basé sur un codage par substitution mono-alphabétique [4]. Ainsi, des travaux récents pour la sécurisation des données images ont été orientés vers la conception des nouveaux algorithmes qui assurent une sécurité fiable tout en minimisant le coût de temps de calcul et la perte d’information.

Je propose dans mon étude une nouvelle méthode de cryptage d’image qui a été proposée basée sur la matrice House Holder, pour éliminer la complexité de calculé l’inverse de la clé de déchiffrement, ainsi, facilite la transmission de cette clé. Aussi, elle utilise une technique de permutation des pixels pour assurer les propriétés de la confusion et la diffusion, pour chiffrer les images qui contiennent des grandes zones d'une couleur unique [3].

Pendant les deux années précédentes plusieurs articles médicaux et sociaux ont été réalisée suite a l’épidémie Covid 19, et parmi eux j’ai lu un qui ma intriguer {Les données médicales de 500 000 Français dérobées et diffusées sur internet} publiée par [Ouest-France](https://www.ouest-france.fr/)  le 23/02/2021 , ce qui m'a poussé à m'intéresser plus particulièrement sur comment sécuriser les images médicales durant leurs transfert dans les canaux de communication

De nos jours les images médicales (comprenant des scanners et des IRM) font certainement partie des données numériques les plus sensibles et personnelles. Pour autant, ce sont vulnérables et faciles à pirater puisque le transmet se fait d’une façon non sécurisée sur des canaux de communication.