Faculté des Sciences et Techniques

Département d'Informatique

MST SIDI -Module: SSI – A.U 2022/2023

Mini Projet : compression et cryptage des vidéos

Filière : 1ère année Master en Système d'information Décisionnel et Imagerie (SIDI)

[redacted]

[redacted]

[redacted]

[redacted]

I. Introduction :

Le développement exponentiel des systèmes de télécommunications a permis le déploiement de certains services sur internet comme la visioconférence ou les plateformes de vidéo en ligne, de plus avec l'arrivée de l'internet des objets, le nombre des flux vidéo devient de plus en plus énorme.

Dans ce mini_projet, nous examinerons une application, sous python, de compression et de cryptage des vidéos utilisant l'algorithme Discrete Wavelet Transform (DWT) pour la compression et l'Advanced Encryption Standard (AES) pour le cryptage. Cette application permet de sécuriser les fichiers vidéo tout en les réduisant de taille.

En outre, dans cette étude, nous avons évalué la qualité de la compression des vidéos en utilisant la DWT en utilisant des mesures de qualité telles que le Peak Signal-to-Noise Ratio (PSNR), le Mean Squared Error (MSE) et le Structural Similarity Index (SSIM). Nous avons également évalué la qualité du cryptage des fichiers vidéo en utilisant l'histogramme, l'entropie et le coefficient de corrélation.

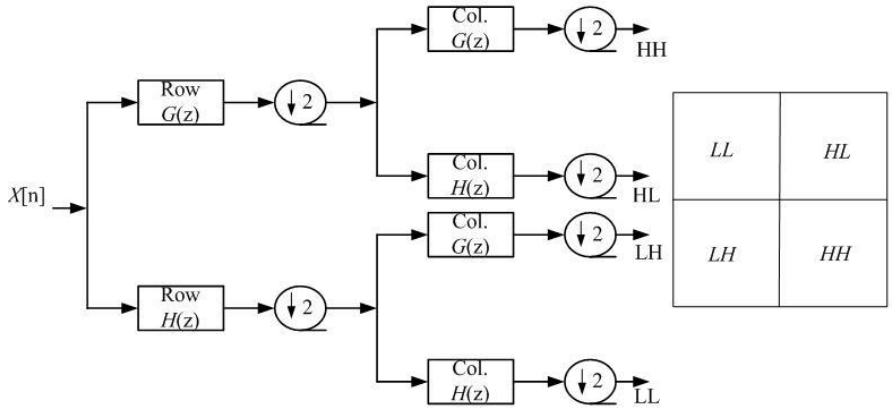
II. Les algorithmes utilisés dans l'application :

1. Discrete Wavelet Transform (DWT) :

La compression par ondelettes, aussi appelée DWT (Discrete Wavelet Transform) est une méthode basée sur la théorie mathématique de l'analyse du signal : les ondelettes sont un ensemble de signaux élémentaires à partir desquels on peut reconstruire un signal complexe. La compression par ondelettes consistera donc à décomposer l'image perçue comme un signal en un ensemble d'images de plus petite résolution. Ce procédé, qui repose sur la différence entre zones de contrastes forts et zones de contrastes faibles, se développe en trois phases :

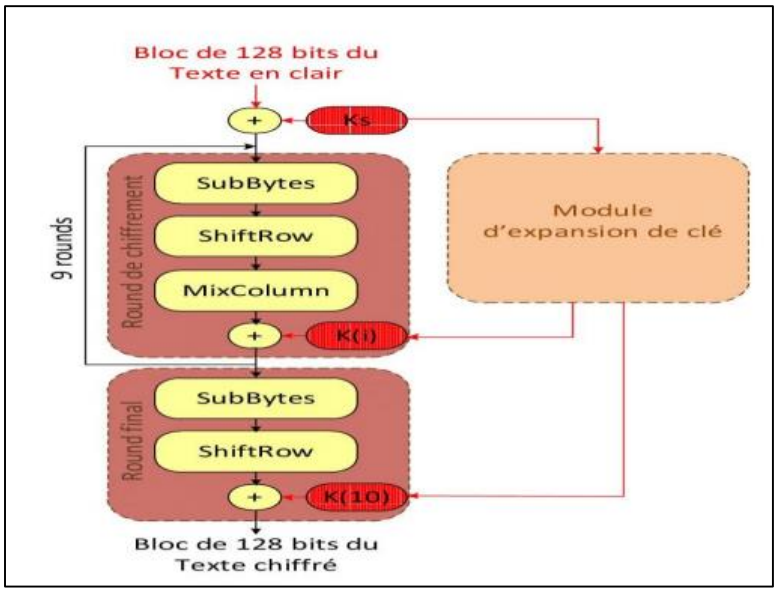
- Tout d'abord, on procède à une transformation de l'image en ondelettes selon un schéma à plusieurs niveaux, processus relativement complexe qui est détaillé ci-dessous.
- Ensuite, on réalise une quantification des informations. Lors de cette phase, les détails qui se situent au-dessous d'un certain seuil sont purement et simplement éliminés. C'est donc à ce niveau que se produit la perte d'informations.
- Enfin, on termine en codant les informations.

La décompression des images s'opère par le schéma inverse : les informations sont tout d'abord décodées pour fournir un ensemble à plusieurs niveaux d'ondelettes qui permettent la reconstitution progressive de l'image.



2. Advanced Encryption Standard (AES) :

AES est un algorithme symétrique de chiffrement par blocs utilisé dans le monde entier sur des supports matériels et logiciels pour protéger les données sensibles.

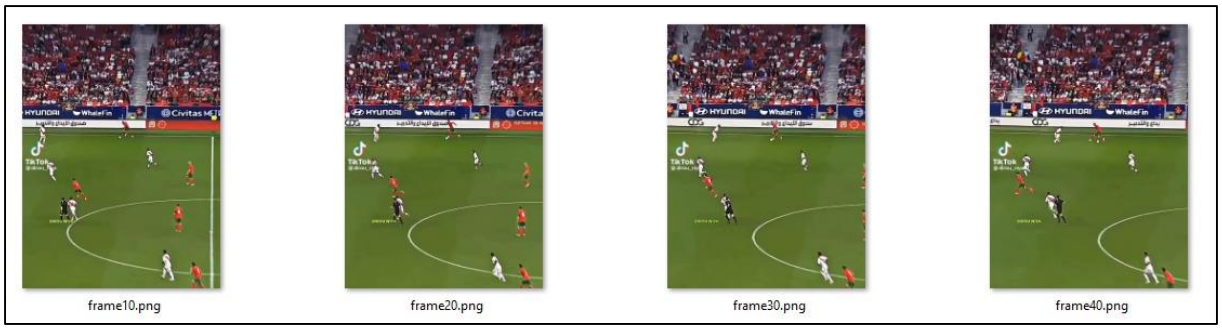


III. Application :

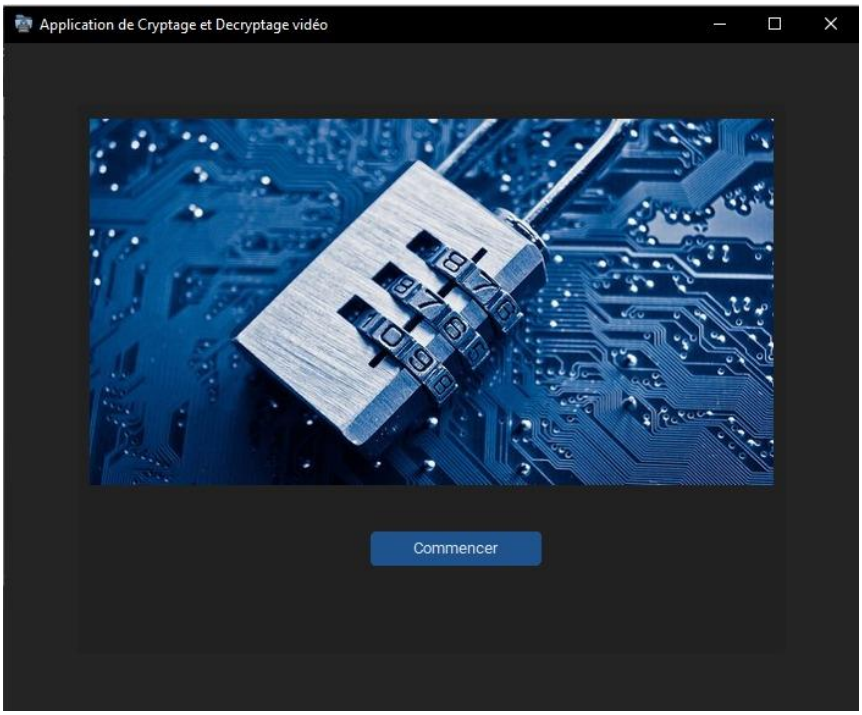
Pour créer l'interface graphique de notre application on a utilisé la bibliothèque « customtkinter » de python qui offrir une interface moderne plus que celle de tkinter. Par la suite, on va analyser les performances de compression (MSE ,PSNR ,SSIM),et de cryptage en utilisant l'histogramme, l'entropie et le coefficient de corrélation.

1) La vidéo utilisée :

Afin de tester le bon fonctionnement de notre interface, nous avons utilisé une vidéo d'une durée d'une seconde. Nous avons ensuite sélectionné uniquement quatre images à partir de cette vidéo, en éliminant toutes les autres. Cette démarche nous a permis de vérifier si notre interface était en mesure de traiter efficacement les images sélectionnées et de fournir les résultats attendus.



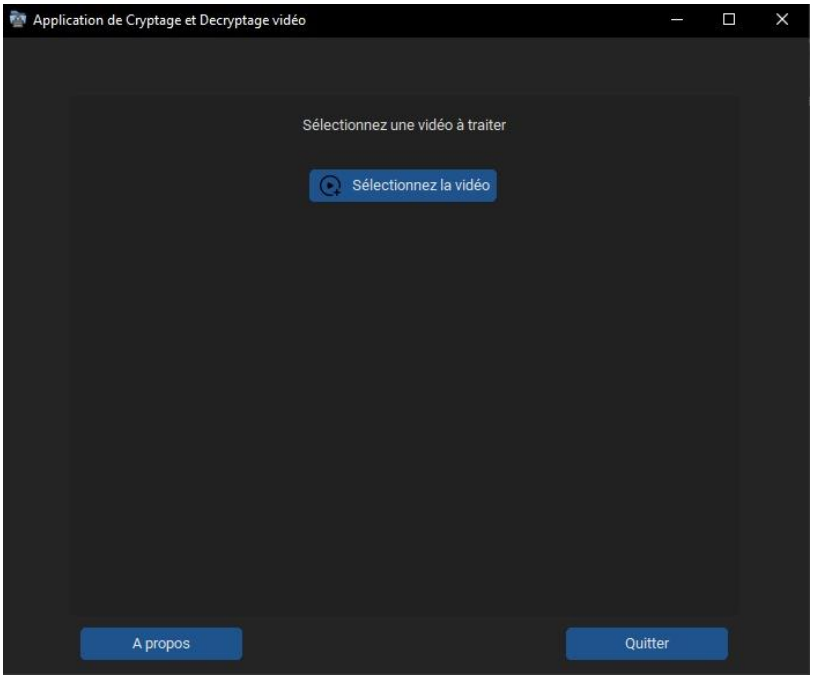
2) Interface d'accueil:



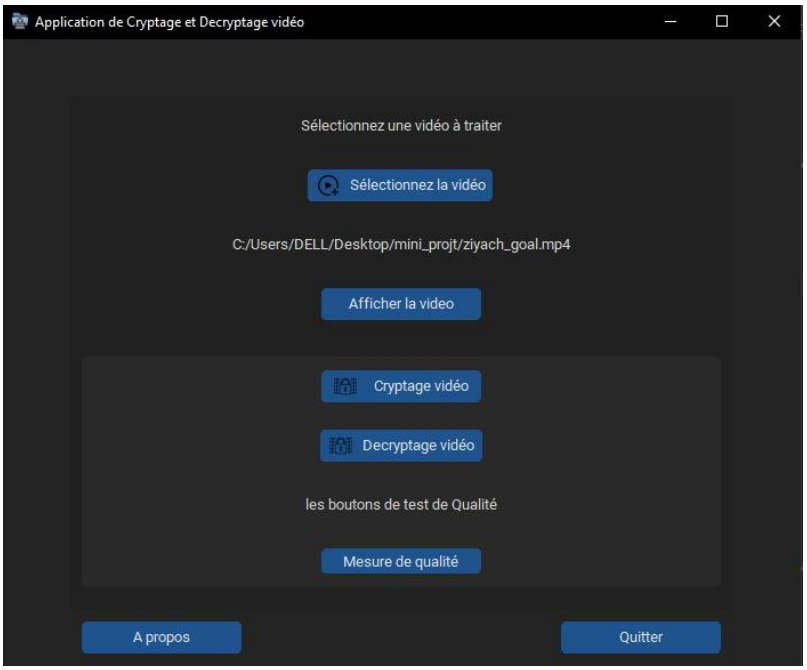
Lorsqu'un utilisateur clique sur le bouton "Commencer", une nouvelle interface s'affiche. Cette interface contient un bouton permettant à l'utilisateur de sélectionner la vidéo qu'il souhaite traiter. L'application supporte tous les types de vidéo et accepte des tailles différentes.

De plus, cette interface propose également un bouton "A propos", qui fournit une description du mode de fonctionnement de l'application. Enfin, il y a un bouton "Quitter" qui permet à l'utilisateur de sortir de l'application.

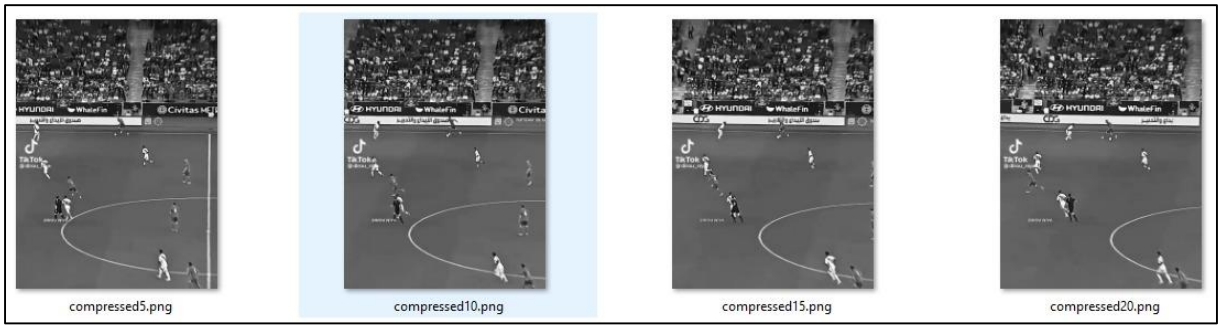
3) Les autres interfaces :



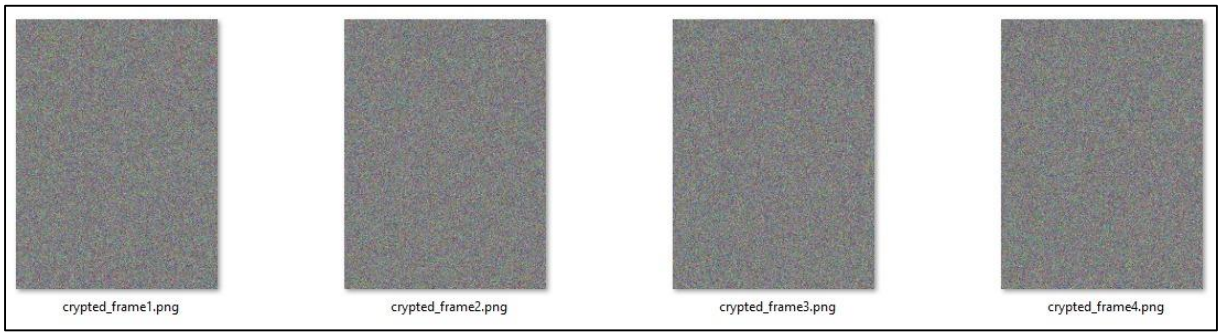
Après avoir sélectionné la vidéo, l'interface affiche de nouveaux boutons, notamment "Cryptage", "Décryptage", "Afficher la vidéo" et "Mesure de qualité". Le premier bouton permet de découper la vidéo en images, puis de les compresser en utilisant l'algorithme DWT. Ensuite, ces images compressées sont cryptées par l'algorithme AES.Le deuxième bouton est utilisé pour décrypter les images précédemment cryptées, puis les décompresser. Le troisième bouton permet d'afficher la vidéo originale, tandis que le dernier bouton affiche un ensemble de mesures sous forme de chiffres. Ces mesures permettent de déterminer la qualité de la compression et du cryptage.En outre, le chemin de la vidéo sélectionnée s'affiche dans une zone spécifique de l'interface.



Le résultat compression des quatre images et donner comme suit :



Et le résultat de cryptage par AES est le suivant :



Les mesures de qualité :

```
{'compressed10.png': {'PSNR': 37.07082039866995, 'MSE': 12.764338740596065, 'SSIM': 0.9922722599976018}}
{'compressed10.png': {'PSNR': 37.07082039866995, 'MSE': 12.764338740596065, 'SSIM': 0.9922722599976018}, 'compressed15.png': {'PSNR': 37.13558907819103,
{'compressed10.png': {'PSNR': 37.07082039866995, 'MSE': 12.764338740596065, 'SSIM': 0.9922722599976018}, 'compressed15.png': {'PSNR': 37.13558907819103,
{'compressed10.png': {'PSNR': 37.07082039866995, 'MSE': 12.764338740596065, 'SSIM': 0.9922722599976018}, 'compressed15.png': {'PSNR': 37.13558907819103,
@ 6.526301
@ 7.631836
@ 6.5021205
@ 7.630795
@ 6.4764457
@ 7.632365
@ 6.5765543
@ 7.631654
histogram_diff 0.23642304072324802 entropy_diff 1.111307144165039 corr_coef_diff 0.0089227333759637114
```

4) Les mesures de performances (compression et cryptage):

Mean Square Error (MSE) : l'erreur quadratique moyenne

C'est une méthode, d'évaluation de la qualité d'image, avec référence complète c.-à-d qu'elle a un accès à une version parfaite de l'image avec lesquelles il peut comparer la version dégradée. L'image dégradée Î est toujours comparée à l'originale I pour déterminer son rapport de ressemblance. Il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et dégradés : Où (M × N) est la taille de l'image

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} \left(I(m,n) - \hat{I}(m,n) \right)^2$$

Peak Signal to Noise Ratio (PSNR) : le rapport crête signal sur bruit

Est une mesure de distorsion utilisée en image numérique. Elle permet de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale, elle est une fonction de MSE

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^{\ 2}}{MSE}\right)$$

Pour une image à niveau de gris, Imax désigne la luminance maximale possible.

Structural Similarity (SSIM) : Indice de similarité structurelle

SSIM est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale. L'idée de SSIM est de mesurer la similarité de structure entre les deux images, plutôt qu'une différence pixel à pixel.

La métrique SSIM est calculée sur plusieurs fenêtres d'une image. On dénote x et y l'image originale et l'image déformée respectivement.

$$SSIM(x,y) = l(x,y).c(x,y).s(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)(cov_{xy} + c_3)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)(\sigma_x\sigma_y + c_3)}$$

l(x, y) :La fonction de comparaison de luminance.

c(x, y) :Le contraste entre deux fenêtres , comparent les variances de x et y.

s(x, y) :La troisième fonction compare les structures des deux fenêtres.

- μ_x, μ_y la moyenne de x et y ;
- σ_x, σ_y la variance de x et y ;
- cov_{xy} la covariance de x et y ;
- $c_1=(k_1L)^2$, $c_2=(k_2L)^2$ et $c_3=c_2/2$ trois variables destinées à stabiliser la division quand le dénominateur est très faible ;
- L : la dynamique des valeurs des pixels, soit 255 pour des images codées sur 8 bits ;
- k_1 = 0,01 et k_2 = 0,03 par défaut.

L'histogramme :

En imagerie numérique, l'histogramme est la représentation graphique de la distribution des pixels d'une l'image, ou d'une partie d'image, selon leur intensité. La forme la plus classique répartit la plage d'intensité sur l'axe horizontal, le noir ou les tons sombres étant situés à l'origine du graphique.

Entropie de Shannon :

L'entropie de Shannon est une mesure de quantité d'information utilisée pour évaluer le caractère aléatoire de la distribution des pixels d'une image chiffrée :

$$H(I) = -\sum_{k=0}^{2^l-1} P(\alpha_k)\log_2(P(\alpha_k)),$$

où I est une image de m × n pixels codés sur 2^l valeurs α_k ($0 \le k < 2^l$) et $P(\alpha_k)$ est la probabilité associée à α_k. La valeur de l'entropie est exprimée en bits-par-pixel (b_{pp}) et comprise entre 0 b_{pp} et $\log_2(2^l) = l$ b_{pp}, lorsque la distribution des pixels est parfaitement uniforme. En général, les images en niveaux de gris sont codées sur 256 valeurs. Dans ce cas, l'entropie maximale est alors de $\log_2(256) = 8$ b_{pp}. Ainsi, la valeur de l'entropie d'une image chiffrée doit être très proche de la valeur de l'entropie maximale.

Coefficient de corrélation :

Une métrique classique consiste à observer la corrélation entre les pixels dans les directions horizontale, verticale et diagonale. M paires de pixels voisins (x_i , y_i) dans les trois directions, avec $x_i \in x$ et $y_i \in y$, sont ainsi choisies pour le calcul du coefficient de corrélation :

$$corr_{x,\,y} = \frac{\frac{1}{M}\sum_{i=1}^{M}(x_i - E(x)) \times (y_i - E(y))}{\sqrt{\frac{1}{M}\sum_{i=1}^{M}(x_i - E(x))^2}\sqrt{\frac{1}{M}\sum_{i=1}^{M}(y_i - E(y))^2}}.$$

où E(x) est la moyenne de l'ensemble x. La valeur de ce coefficient de corrélation est comprise en −1 et 1, où −1 et 1 indiquent une forte corrélation et 0, l'absence de corrélation. Comme les valeurs des pixels voisins dans le domaine clair sont fortement corrélées, $corr_{x,y}$ est généralement élevé dans l'image originale en clair. En revanche, il doit être proche de zéro dans le domaine chiffré.

IV. Conclusion :

Dans ce rapport, nous avons présenté les principales fonctionnalités de notre application, qui permet de crypter et décrypter des vidéos après compression. Nous avons fait de notre mieux pour répondre aux exigences du projet, mais nous avons rencontré plusieurs obstacles qui nous ont empêchés d'atteindre tous nos objectifs.

Notre application est capable de compresser des vidéos et de crypter les images compressées en utilisant des algorithmes DWT et AES. Cependant, la fonctionnalité de décompression n'est pas encore opérationnelle et nécessite des améliorations.