## Université Paris-Saclay Master 1 d'Informatique Introduction à l'apprentissage automatique

# RECONNAISSANCE D'IMAGE

AKHARAZ MAJID



01-05-2020

# Contents

1	Introduct	ion	1	
2	Méthode du plus proches voisins.			
	2.0.1	Définition formelle de l'algorithme du plus proche voisin:	4	
	2.0.2	Implémentation:	5	
3	Méthode	des K plus proches voisins.	8	
	3.0.1	Définition formelle de l'algorithme des K plus proches voisins:	8	
	3.0.2	Stratégie de recherche pour le choix de K et de la Distance:	8	
	3.0.3	L'implémentation:	9	
4	Conclusio	n.	11	
5	Implémentation de l'article intitulé: An Analysis of Single Layer Networks in Unsupervised Feature Learning.			
	5.0.1	Définition des concepts :	12	
	5.0.2	Construction de notre modèle :	13	
	5.0.3	Résultat:	15	
	5.0.4	Problèmes rencontrés	17	
	5.0.5	Amélioration possible	17	
6	Conclusio	n finale.	19	

# 1. Introduction

Motivation: Classification d'images

La classification d'images est un problème central en vision par ordinateur, ayant de nombreuse applications concrètes. L'objectif est de construire un système ayant la capacité d'assigner à n'importe quelle image d'entrée une catégorie.

Evidémment un ordinateur ne peut pas voir une image comme un humain. Pour l'oridnateur une image couleur, est représentée par une matrice tridimensionnelle. Dans l'exemple ci dessous, le chien est réprésenté par une image de 64 pixels de hauteur et 64 pixels de largeur, sur lesqulles chaque pixels est représenté par 3 entiers, un entier pour le rouge un autre pour le vert et un dernier pour le bleu. Ainsi une image de  $64 \times 64$  est, pour l'ordinateur, représenté par:  $64 \times 64 \times 3 = 12288$  entiers. Notre objectif est de donner un sens à ces 12288 nombre de telle sorte que l'ordinateur puisse nous retourner la catégorie d'appartenance de l'image en entrée.

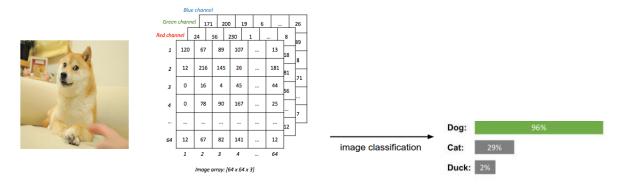


Figure 1.1: L'objectif est de prendre en entrée une image et de lui associer une "étiquette" (ou plusieurs étiquettes auxquelles on associe un probabilité de vraisemblance).

#### Difficulté:

Une telle têche est trivial pour un humain, mais qu'en est il pour un ordinateur? Nous détaillons ici quelques pistes permettant de comprendre pourquoi l'élaboration d'un algorithme de classification d'image peut présenter de réel difficulté.

- Les différences d'un même groupe: Des objets d'une même classe peuvent présenter des différences considérable.;
- L'arrière plan de la photo: Il peut arriver que l'arrière plan de la photo se confondent avec l'image;

- Différence de luminosité: La coloration des pixels peut considérablement changer en fonction de la luminosité.
- La non complitude de l'objet sur l'image: Il est possible que l'objet qui nous intéresse soit rogner sur l'image, qu'on puisse en voir qu'une partie.
- Déformation: L'objet d'interêt peut etre très souple, non rigide. Cela pourrait entrainer des déformations.
- Différence de taille: Un même objet représenter d'une taille différente.
- Le point de vue: Un objet de face et un objet de profil sont "vue" différement pour un ordinateur.

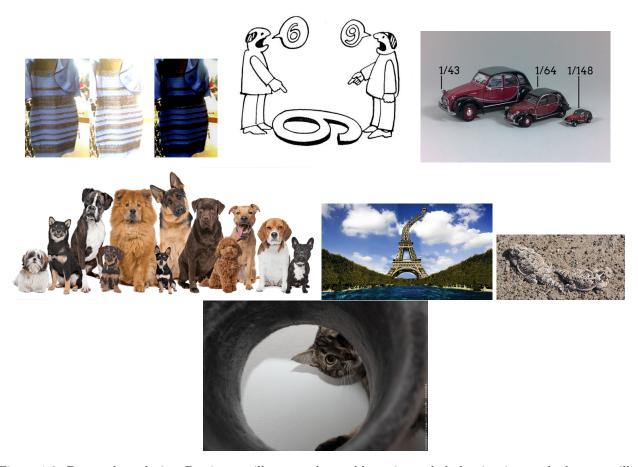


Figure 1.2: De gauche à droite: Des images illustrants les problèmatiques de la luminosité, angle de vue, taille de l'image, différence d'objet du même groupe, déformation de l'object, un arrière plan confondu avec l'image, et enfin une image dont l'objet est que partiellement apparent

### Pourquoi attaquer ce problème avec l'apprentissage automatique:

Ainsi on se questionne sur savoir comment créer un algorithme qui pourrait classer chaque image dans la catégorie qui lui correspond sachant que pour l'ordinateur une image n'est qu'une liste de nombre?

La difficulté est qu'il nous ait impossible de répertorier exhaustivement les caractéristique d'un chat, d'une voiture, d'un chien le tout dans des contextes qui peuvent altérer ces caractéristiques.

Dès lors, nous allons donc fournir à l'ordinateur de nombreux exemples de chaque catégorie, puis développer des algorithmes d'apprentissage capable d'analyser « regarder » ses exemples et assimiler assez de connaissance pour apprendre qu'elle est l'apparence visuelle de chaque catégorie.

Cette approche est donc basée sur les données, puisqu'elle repose sur l'accumulation d'un grands nombre de données dit d'apprentissage.

#### Les données utilisées pour ce projet:

Dans le cadre de ce projet nous utiliserons un ensemble de donnée appelé CIFAR-10. Cette base de donnée comprends 60 000 petites images de dimension  $32 \times 32$ . Chaque image est labelisé par une des 10 catégories (avion, voiture, oiseau, etc) présentent dans la base. Les 60 000 images sont partitionnées en deux catégories:

- 50 000 images d'entrainement.
- 10 000 images de testes.



Pour accomplir notre tache nous explorerons plusieurs méthodes, nous tenterons d'aborder des approches considéré comme étant de plus en plus sophistiqué, nous avons pour ambition de detailler ces différentes approches et de les expliquer autant que faire ce peut.

# 2. Méthode du plus proches voisins.

Dis moi qui est ton voisin je te dirais qui tu es.

**Information:** Les data étant trop volumineuses pour être traité par nos ordinateurs, nous avons choisit de faire "tourner" nos algorithmes sur des échantillons réduits. 5000 images d'entrainement et 500 de tests.

Cette méthode consiste à prendre succéssivement toutes nos images de test et à mesurer la dissimilarité avec chacune des images de notre ensemble d'entrainement. Ici pour notre ensemble de données, il s'agit de calculer la dissimilarité de chacune de nos 10 000 images, avec chacunes des 50 000 images, on se rends tout de suite compte de deux choses. Cette méthode est facile à implémenter mais est très couteuse en temps de calcul lorsque le nombre d'objet devient très grand.

Pour calculer cette dissimilarité, nous calculons la différence entre chaque pixel des matrices en question. Nous avons fait le choix de prendre comme distance la distance  $L^1$ , formellement cette distance s'écrit comme suit, soit deux images représenté par deux vecteur  $X_1$  et  $X_2$ :

Distance  $L^1$ :

$$d_1(X_1, X_2) = \sum_i |X_1^i - X_2^i|$$

#### 2.0.1 Définition formelle de l'algorithme du plus proche voisin:

Soit  $X = (x_1, ..., x_N) \subset E$  un ensemble d'éléments d'un espace métrique quelconque, soit  $(c(x_1), ..., c(x_N))$  les classes associées à chacun des éléments de X. On note d la distance définie sur l'espace métrique (Un espace que l'on peut munir d'une norme) E. Soit x un élément à classer, on cherche à déterminer la classe  $\hat{c}$  associé à x. On définit  $x_i^*$  comme étant:

$$x_i^* = \operatorname*{arg\,min}_{i \in \{1, \dots, N\}} d(x_i, x)$$

Alors  $\hat{c}(x) = c(x_i^*)$ 

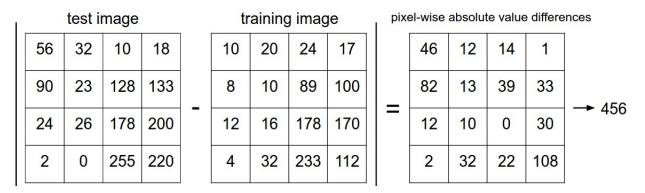


Figure 2.1: Ici nous représentons un exemple simplifié (une seule couleur) de l'utilisation du calcul de dissimilarité par utilisation de la distance  $L^1$ . Deux images sont soustraites pixel par pixel, puis nous additionner l'ensemble des soustractions, cet entier est la distance entre les deux images. Ainsi si deux images sont identiques la somme de leurs différences est zero. A contrario si les images sont très differentes le resultat sera grand.

### 2.0.2 Implémentation:

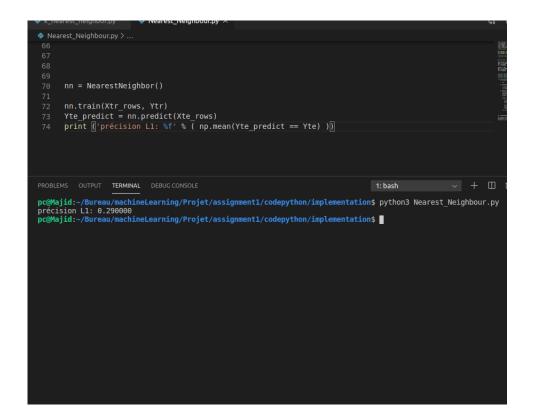
Dans un premier temps, nous chargons Cifar10 avec la fonction loadcifar10() en mémoire dans 4 tableaux: Xtr est toutes les données d'entrainement ce tableau est de taille  $(50000 \times 32 \times 32 \times 3)$ . Ytr est un vecteur de taille  $50\ 000\ qui$  contient tous les labels de  $0\ à\ 10$ .

Puis avec la fonction **reshape** on redimensionne les tableaux de telle manière à representer les images en lignes. Ce traitement des données étant fait, il ne reste plus qu'à entrainer notre modèle avec la fonction **train**, dans le cadre du plus proche voisin, l'entrainement consiste simplement à mettre en mémoire. Ensuite vient l'étape de prédiction avec la fonction **predict()**, cette fonction, pour chaque image test calule sa distance avec toutes les images d'entrainement, et retiens la distance la plus petite distance ainsi que l'indice du label.

Nous évaluons l'éfficaté de notre algorithme en calculant le ratio :

$$\mathbf{Efficacit\acute{e}} = \frac{\text{Nombre de bonne pr\'ediction}}{\text{Nombre total de pr\'ediction}}$$

Notre algorithme naïf présente une précision de 29%. Les images toujours mal prédite sont celle avec les fond de couleurs homogènes. On explique cela par le fait que les images ayant les memes nuances de couleur en arrière plan, minimise la dissimilarité, et ceux même si notre objet d'intérêt est totalement différent.

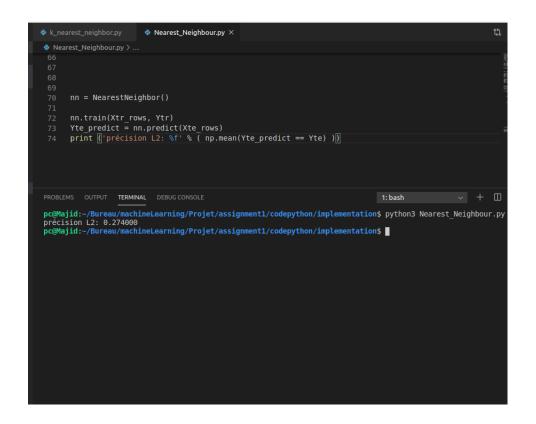


Une telle méthode n'a pas de rempart contre les valeurs abberantes. Nous essayons la distance  $L^2$  pour avoir une idée du résultat:

### Distance $L^2$ :

$$d_1(X_1, X_2) = \sqrt{\sum_i |X_1^i - X_2^i|^2}$$

Nous obtenons un résultat infieur à celui de L1 de 27%.



# 3. Méthode des K plus proches voisins.

Dis moi qui sont tes voisins je te dirais qui tu es.

L'idée est assez proche de celle du plus proche voisin, sauf qu'au lieu de trouver l'image la plus proche, nous chercherons à trouver les  $\mathbf{K}$  images les plus proches, puis parmis ces  $\mathbf{K}$  images nous regardons la classe qui revient le plus souvent, c'est cette dernière que nous étiqueterons nous image test.

Ainsi lorsque K=1, nous sommes exactement dans un problème du plus proche voisin.

#### 3.0.1 Définition formelle de l'algorithme des K plus proches voisins:

Soit  $X=(x_1,...,x_N)\subset E$  un ensemble d'éléments d'un espace métrique quelconque, soit  $(c(x_1),...,c(x_N))$  les classes associées à chacun des éléments de X. On note d la distance définie sur l'espace métrique (Un espace que l'on peut munir d'une norme(distance)) E.  $\omega(x,y)$  est une fonction strictement positive mesurant la ressemblance entre x et y. Soit x un élément à classer, on cherche à déterminer la classe  $\hat{c}(x)$  associée à x. On définit l'ensemble  $S_k^*$  incluant les k-plus proches voisins de x, cet ensemble vérifie:

$$\mathrm{Card} S_k^* = k \ et \ \max_{y \in S_k^*} d(y,x) \leq \min_{y \in X - S_k^*} d(y,x)$$

On calcule les occurences f(i) de chaque classe i dans l'ensemble  $S_k^*$ :

$$f(i) = \sum_{y \in S_k^*} \omega(x, y) \mathbb{1}_{\{c(y) = i\}}$$

On assigne alors à x la classe c(x) choisie dans l'ensemble:

$$\hat{c}(x) \in \operatorname*{arg\,max}_{i \in \mathbb{N}} f(i)$$

L'une des premières questions que l'on se pose lors de l'implémentation de cet algorithme est le choix de K.

### 3.0.2 Stratégie de recherche pour le choix de K et de la Distance:

Le nombre K et la distance sont des **Hypeparamètres**. Pour choisir le bon K et la bonne distance, nous avons choisit une stratégie naïve qui consiste à essayer plusieurs distance et plusieurs K et garder ceux qui offrent les meilleurs résulats.

Le problème qui s'est posé à nous est que nous ne pouvions pas utiliser l'ensemble de test pour ajuster nos paramètres, le risque de cela aurait été de paramétré notre en algorithme en fonction du jeu de test que nous avons, cela rendrer notre algorithme totalement innéficace sur un autre jeu de test.

La strategie mise en place consiste à divisier nos données d'entrainements, nous gardons 49 000 images pour l'entrainement et 1000 pour la validation des paramètres, en utilisant la méthode de corss-validation.

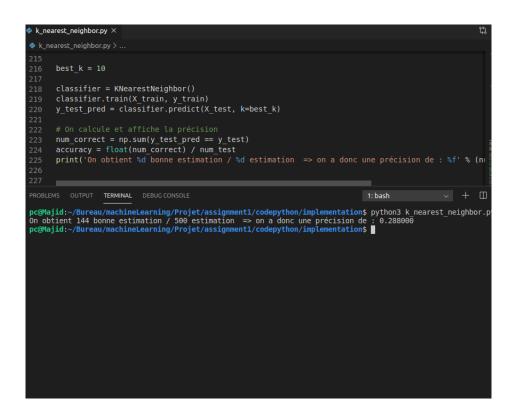
### 3.0.3 L'implémentation:

Nous procédons en deux étapes:

- On calcule toutes les distances entres les données de test et celle d'entrainement;
- Ayant ces distances, pour chaque donnée de test on trouve les K plus proches images et on effectue la selection du label en fonction du nombre de label le plus présent parmis les K;

```
(500), 3072) (500), 3072)
k = 1, accuracy = 0.253000
k = 1, accuracy = 0.253000
k = 1, accuracy = 0.254000
k = 3, accuracy = 0.256000
k = 3, accuracy = 0.253000
k = 3, accuracy = 0.255000
k = 5, accuracy = 0.255000
k = 6, accuracy = 0.255000
k = 8, accuracy = 0.255000
k = 8, accuracy = 0.255000
k = 8, accuracy = 0.255000
k = 10, accuracy = 0.255000
k = 10, accuracy = 0.255000
k = 10, accuracy = 0.255000
k = 11, accuracy = 0.255000
k = 12, accuracy = 0.255000
k = 11, accuracy = 0.255000
k = 12, accuracy = 0.255000
k = 12, accuracy = 0.250000
k = 13, accuracy = 0.250000
k = 14, accuracy = 0.250000
k = 15, accuracy = 0.250000
k = 15, accuracy = 0.250000
k = 15, accuracy = 0.250000
k = 16, accuracy = 0.250000
k = 17, accuracy = 0.250000
k = 18, accuracy = 0.250000
k = 19, accuracy = 0.250000
k = 10, accuracy = 0.250000
k = 10, accuracy = 0.250000
k = 20, accuracy = 0.2500000
k = 20, accuracy = 0.2500000
k = 20, accuracy = 0.250000000000000000000000000000000
```

En choisissant le meilleur K d'après le test sur les hyperparamètres nous obtenons une pourcentage de réussité de 28% ce qui est, de manière contre-intuitive, inférieur à l'algorithme du plus proche voisin.



# 4. Conclusion.

Les algorithmes de plus proches voisins présentent l'avantage d'être facile à comprendre cependant leurs performances restent très relatifs. En effet, le calculs de dissimilarité par distance des pixels, présentent de nombreux inconvénient (différentes nuances de couleurs d'un objet d'une même classe, arrière plan de couleur identifque de deux objets de même classe etc ...) difficient à résoudre.

# 5. Implémentation de l'article intitulé: An Analysis of Single Layer Networks in Unsupervised Feature Learning.

Remarque: Nous nous sommes globalement aidé des deux sources internet que sont [1] et [4].

Cette article nous enseigne qu'il est possible d'atteindre des résultats impréssionnant sans utiliser d'algorithme d'apprentissage complexe et sans que le modèle d'apprentissage soit profond.

En effet, l'article affirme qu'il est possible d'atteindre un excellent résultat en jouant sur deux critères essentiels, le nombre de noeud dans la couche intermédiaire ainsi que la densité d'extraction des features, à tel point que si ces deux paramètres sont choisis de manière optimal on peut atteindre les meilleurs résultats existants.

### 5.0.1 Définition des concepts :

Dans cette section nous définissons certains concept clé à l'implémentation de l'algorithme présenté dans l'article.

#### Normalisation:

Il s'agit de la soustraction suivante:

$$X^{'} = X - \bar{x}$$

Ou  $X^{'}$  est l'ensemble de donné normalisé, X l'ensemble de donné original et  $\bar{x}$  la moyenne de X. On soustrait au vecteur sa moyenne. Cela aura l'effet de centrer les données autour de 0.

#### Blanchiment:

L'objectif du blanchiment est de supprimer les corrélations entre pixel afin de forcer l'algorithme à se concentrer sur des données pertinentes.

$$X = U.diag(\frac{1}{\sqrt{diag(S) + \varepsilon}}).U^T.X$$

Avec U le vecteur singulier gauche et S les valeures singulières de la covariance des données initial après normalisation.  $\epsilon$  est un hyper-parametre appelé coefficient de blanchiement. diag(S) est une matrice acec le vecteur S en diagonal et 0 ailleur.

#### Features:

Les features sont le resultat de la transformation numérique des caractéristiques que l'algorithme devra analyser pour faire ces prédictions. On obtient ces features par des calculs plus ou moins complexe. Les features sont les parties des données qu'on utilise pour faire notre analyse.

#### **Dropout:**

Un procédé qui consiste à detuire aleatoirement des noeuds du reséaux de neuronnes. C'est un procédé ayant pour objectif de diminuer la différence entre les erreurs d'entrainement et les erreurs de test (Overfitting).

#### Fonction d'activation:

La fonction d'activation d'un noeud défini la valeur de sortie de ce noeud. Le noeud prend en valeur d'entrée un input qui est transformé en output par la fonction d'activation.

#### Learning rate (taux d'apprentissage):

Le learning rate est un paramètre qui contrôle la quantitée de changement que nous effectuons sur les poids de notre réseau, guidé par la valeur de notre gradient.

#### Momentum:

Pertubation émise lorsque le gradient est égale à 0 pour sortir du "plat".

#### Overfitting:

Le modèle prends en considération des points de nos images qui ne représentent pas réellement les propriétés de l'image en question.

#### Regularization:

Un paramètre qui permet de regulariser la fonction de perte (Loss function) qui parfois a un comportement indésirable. Nous limitons ce comportement en ajoutant un terme de régularisation.

#### 5.0.2 Construction de notre modèle :

#### Paramétrisation:

Dans cette section nous présenterons succintement la méthode utilisé pour optimiser le choix du nombre de neuronnes dans notre unique couche, la méthode utilisé est celle dite de "Grid search" il s'agit, comme dans la première partie du rapport, de tester différentes combinaison possibiles pour nos paramètres. Nous avons utilisé cette méthode pour fixer 3 paramètres qui sont:

- Nombre de neuronnes;
- Taux d'apprentissage (Learning rate);
- La force de regularisation.

Les différents résultats obtenus nous ont permis d'obtenir un score de 51% avec le paramétrage suivant: 350 neuronnes, un taux d'apprentissage de 0.001 et une force de régularisation de 0.05.

Pour y parvenir nous avons utilisé une exploration du nombre de noeuf allant de 150 à 550 avec un saut de 50.

Pour le taux d'apprentissage nous avons exploré toutes les possibilités entre  $1e-3*10^{-3}$  à  $1e-3*10^{3}$ . avec un ratio de 10.

Et pour la force de régularisation nous avons exploré toutes les possibilités entre  $0.5 * 10^{-3}$  à  $0.5 * 10^{3}$  avec un ratio de 10 aussi.

#### Preprocessing:

Avant de lancer l'entrainement sur les données nous les avons traités en utilisant deux méthodes. L'analyse en compostante principal afin de blanchir les données en effectuant une decorrélation des imagés en entrée et supprimer les informations redondantes. Ensuite nous utilisons un algorithme de clustering par K-means avec 1600 centroïdes.

Cette étape accélère l'extraction des features et augemente la qualité des prédictions.

#### Passage en arrière Forward pass et fonction de perte:

L'objectif étant de trouver les bons changements de poids dans la matrice W et de biais dans le vecteur b. Nous avons, pour se faire défini une fonction d'erreur qui, durant l'entrainement compare le resultat de notre modèle avec la valeur exact, notre objectif est des lors de **minimiser** cette **fonction d'erreur (loss function)**.

Comme fonction d'activation, nous avons utilisé la foncton Relu pour éviter les problèmes de saturation qui se présente comme suit:

Fonction ReLu [2] 
$$f(x) = max(0, x)$$

Si l'entrée est négative la sortie est 0 si elle est positive la sortie est x.

Construction de la fonction de perte :

Somme pondéré = 
$$np.max(X.dot(W1) + b1, 0)$$
  
Score = Somme pondéré. $dot(W2) + b2$   
Score expo =  $exp(Score)/(np.sum(exp(Score, 1)).T$ 

### fonction de perte:

```
loss=-np.sum(np.log(Score\ expo[range(len(Score\ expo)),y]))/
len(Score\ expo)+\ 0.5*req*(np.sum(np.power(W1,2))+np.sum(np.power(W2,2)))
```

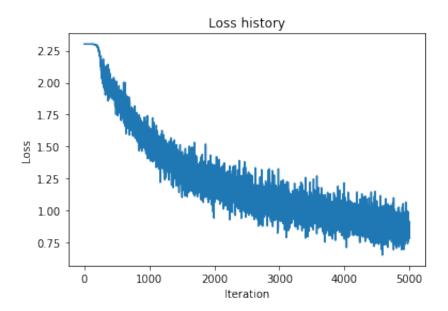


Figure 5.1: Décroissance de la fonction de perte, pour converger à 0.75

#### Dropout: [3]

Puisque nous avons seulement une seule couche le dropout a seulement besoin d'être effectué une seule fois par echantillon d'image d'entrainement (batch).

Comme dit plus haut, nous faisons cela pour éviter l'overfitting. Pour avoir un bon paramétrage du bon nombre de noeud en fonction du dropout nous sommes avec un nombre de noeud plus conséquant (500) puis avec un taux de relachement de 30,50 puis 70%. Cette méthode nous permet de monter à un résultat de 56% de reconnaissance sans de difference entre les différents taux.

Durant nos tests nous n'avons pas vraiment réussi à minimiser l'overfitting nous pensons que nos résultats sont inférieurs à ceux de l'article à cause de cela.

#### 5.0.3 Résultat:

Comme mentionné plus haut nous avons utilisé la méthode de grid search pour trouver les meilleures hyperparamètres. L'un des inconvénients non négligeable que nous avons rencontré pour trouver les bons paramètres est le temps que cela met, une solution à ce problème aurait été peut être d'implémenter l'article aurait été de passer sur Pytorch pour faire les calculs facilement sur GPU.

Il y'a des paramètrages qui n'ont pas pu se terminer (augmenter le nombre de neuronne, augmenter le nombre d'itération et autre) pour des raisons d'erreurs mémoire.

En somme le paramétrage optimal que nous avons trouvé est le suivant:

Paramétrage optimal trouvé			
Noeuds dans le réseaux	200		
Taux d'apprentissage	$5 \times 10^{-4}$		
Décroissance du taux d'apprentissage	0.98		
Régularisation	0.3		
Fonction d'activation	ReLu		
Itération	70 000		
Taille des Batch	128		
Précision sur les données d'entrainement	93%		
Précision du modèle réels	61.5%		
Temps	59 minutes		

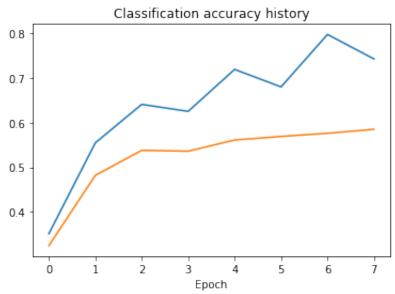
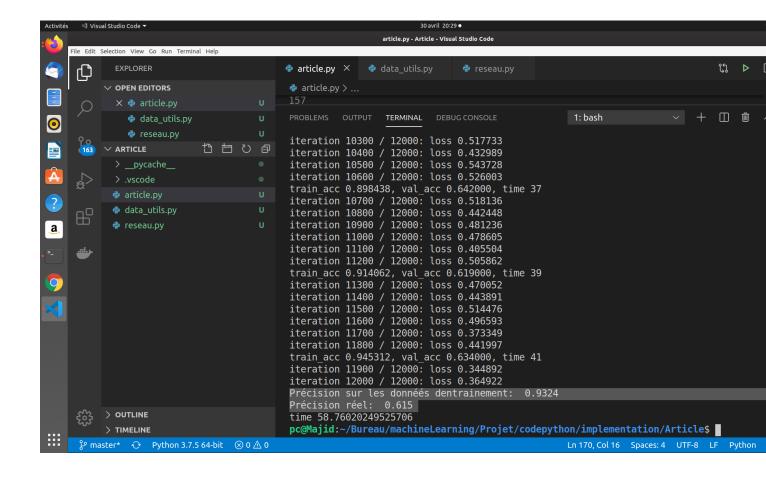


Figure 5.2: en bleu la courbe de reconnaissance des imgages sur le set d'entrainement en orange sur le set de test. 200 noeuds 5 itérations du K-means 5000 itérations d'entrainement



## 5.0.4 Problèmes rencontrés

Nous avons rapidement rencontré des problème de taille (mémoire) et de temps (temps d'execution du code) chaque nouvelle paramétrisation demande une attente d'une heure afin de verifier son efficacité. Aussi malgrès tous nos efforts, nous n'avons pas été en mesure d'atteindre le résultat enoncé dans l'algorithme à ce jours nous pensons que cela est dû à notre echec quant à la minimisation de l'Overfiting.

#### 5.0.5 Amélioration possible

Il existe des fonctions d'activations plus complexe que ReLu notamment ReLu qui pourrait donner de meilleur résultat.

Une utilisation du multi-thread ou du GPU pour augmenter la vitesse calcul, permettrait d'augmenter le nombre de noeud dans la couche ce qui permettrait, je pense, d'obtenir des résultats plus précis. Mais aussi d'augmenter le nombre de degrès de liberté, par exemple agumenter la taille des patches augmenter leurs nombres et augmenter du dropout.

ncernant l'implémentation de l'article je n'utilise que la distance L2 il est possible que la L1 donne dultats.	le meilleur

# 6. Conclusion finale.

Nous n'avions pas considéré à sa juste valeur l'importance des hyperparamètres avec la méthode naïve, en effet ceci était facilement réglable et les combinaisons étaient limité. L'article nous a vraiment permis de considéré les hyperparamètres comment étant des facteurs centraux dans l'efficacité d'un algorithme. Nous avons à présent le sentiment, que l'un des enjeux majeurs lors de la création d'un modèle et de trouver sa bonne paramétrisation.

# Bibliography

- [1] Hadrien. https://hadrienj.github.io/tags/#numpy.
- [2] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification. CoRR, abs/1502.01852, 2015.
- [3] Geoffrey E. Hinton, Nitish Srivastava, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Improving neural networks by preventing co-adaptation of feature detectors. CoRR, abs/1207.0580, 2012.
- [4] trongr. https://trongr.github.io/.