TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH



Môn: Cơ sở trí tuệ nhân tạo

PHÂN LOẠI ẢNH

MÃ MÔN HỌC CSC14003

Thành phố Hồ Chí Minh - 2021

1.	Tổng quan	3
2.	Phân biệt 3 loại training set, validation set, test set:	3
3.	Mô tả cách phát hiện và ngăn chặn overfitting và underfitting problem:	3
3	3.1 Overfitting (quá khớp):	3
3	3.2 Underfitting:	5
4.	Model:	5
5.	Ưu điểm và nhược điểm của model	7
6.	Trình bày kết quả nhận được và giải thích	7
7.	Idea for improvement:	8
8.	Hướng dẫn chạy code	9
9.	Quá trình chạy dữ liệu	12
10	Reference	14

1. Tổng quan

MSSV	HỌ VÀ TÊN	EMAIL		
19127392	Tô Gia Hảo	19127392@student.hcmus.edu.vn		
19127525	Nguyễn Thanh Quân	19127525@student.hcmus.edu.vn		
19127625	Lâm Chí Văn	19127625@student.hcmus.edu.vn		

2. Phân biệt 3 loại training set, validation set, test set:

Training set

Training set: là tập dữ liệu có kích thước lớn, dùng để training cho máy học. Đây chính là tập dữ liệu máy dùng để học và rút trích được những đặc điểm quan trọng để ghi nhớ lại. Tập training set sẽ gồm 2 phần:

- Input: sẽ là những dữ liệu đầu vào

- Output: sẽ là những kết quả tương ứng với tập input

Test set

Test set: là tập dữ liệu dùng để kiểm thử **sau** quá trình huấn luyện. Một mô hình machine learning sau khi được huấn luyện, sẽ cần phải được kiểm chứng xem nó có đạt hiểu quả không. Đây là một tập hợp các giá trị input và được sử dụng để kiểm tra độ chính xác của các mô hình machine learning sau khi được training và đưa ra Ouput tương ứng với mỗi input. Khác với Training set, Testing set chỉ gồm các giá trị input mà không có các giá trị output.

Validation set

Validation test: cũng giống như tập training set, nó cũng bao gồm các cặp giá trị input và ouput tương ứng. Nhưng nó lại khác training set ở chỗ, nó được sử dụng để kiểm thử độ chính xác của mô hình máy học trong quá trình huấn luyện và được sử dụng để kiểm thử **trong** quá trình huấn luyện

3. Mô tả cách phát hiện và ngăn chặn overfitting và underfitting problem:

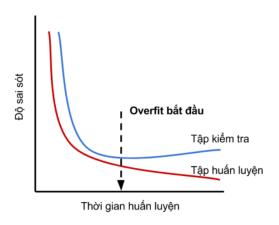
3.1 Overfitting (quá khớp):

Khi mô hình của bạn được training tốt hơn nhiều so với tập validation, nó sẽ ghi nhớ các ví dụ huấn luyện riêng lẻ để mở rộng. Bằng cách đó, nó có thể dự đoán dữ liệu đào tạo của bạn rất tốt, nhưng không khái quát được vấn đề thực tế và do đó thất bại trên các ví dụ không nhìn thấy. Việc khớp dữ liệu đào tạo quá tốt được gọi là Overfitting.

Phát hiện overfitting

Để phát hiện overfitting, ta cần theo dõi **learning curve**, một biểu đồ thể hiện sự biến động của $\mathcal{L}_{D_{train}}$ và $\mathcal{L}_{D_{test}}$ trong suốt thời gian huấn luyện. Cứ sau một khoảng thời gian, ta ghi lại giá trị của $\mathcal{L}_{D_{train}}$ và $\mathcal{L}_{D_{test}}$ và vẽ biểu đồ của chúng theo thời gian, ta được learning curve.

NHÓM 7



- Nếu ta áp dụng một phương pháp tối ưu hàm số hiệu quả, $\mathcal{L}_{D_{train}}$ (đường đỏ) sẽ giảm theo thời gian.
- Ngược lại $\mathcal{L}_{D_{test}}$ (đường xanh) không phải lúc nào cũng giảm. Nếu model bị overfitting, đến một lúc nào đó, gía trị này bắt đầu tăng trở lại.
- Thời điểm mà $\mathcal{L}_{D_{test}}$ bắt đầu có xu hướng tăng được xem thời điểm bắt đầu overfitting. Vì sao? Vì sau đó, việc huấn luyện sẽ làm model dự đoán ngày càng tốt hơn trên training set, nhưng lại cho sai sót ngày càng nhiều trên test set.

Cách để ngăn việc Overfitting:

- Gather more data (Bổ sung nhiều dữ liệu hơn):

Dữ liệu ít là 1 trong trong những nguyên nhân khiến model bị overfitting. Vì vậy chúng ta cần tăng thêm dữ liệu để tăng độ đa dạng, phong phú của dữ liệu (tức là giảm variance). Một số phương pháp tăng dữ liệu:

- + *Thu thập thêm dữ liệu*: chúng ta phải craw thêm dữ liệu hay tới thực tiễn để thu thập, quay video, chụp ảnh,...Tuy nhiên trong nhiều trường hợp thì việc thu thập thêm dữ liệu là infeasible nên phương pháp này không được khuyến khích.
- + **Data Augmentation**: Augmentation là 1 phương thức tăng thêm dữ liệu từ dữ liệu có sẵn bằng cách rotation, flip, scale, skew,... images. Phương pháp này được sử dụng rất phổ biến trong xử lý ảnh cho Deep learning.
- + GAN (Generative Adverserial Network) là mô hình học không giám sát dùng để sinh dữ liệu từ nhiễu (noise)

- Simple model (Mô hình đơn hơn):

model của bạn quá sâu, phức tạp (chẳng hạn như nhiều layer, node) trong khi chỉ có chút xíu dữ liệu, dùng Một mô hình kém mạnh hơn có thể không có khả năng ghi nhớ nhiều ví dụ training, nhưng rất có thể đủ tốt để giải quyết nhiệm vụ của bạn. Nếu bạn sử dụng mạng neutral, hãy thử các lớp nhỏ hơn và ít hơn.

- Regularization(Quy định hóa):

regularization là 1 kĩ thuật tránh overfitting bằng cách thêm vào hàm loss 1 đại lượng **lamda. f(weight)** => Tối ưu model (giảm hàm loss) => giảm weight => mô hình bớt phức tạp => tránh overfitting.

- Use Dropout:

Dropout là kĩ thuật giúp tránh overfitting cũng gần giống như regularization bằng cách bỏ đi random p% node của layer => giúp cho mô hình bớt phức tạp (p thuộc [0.2, 0.5]).

Early stoping:

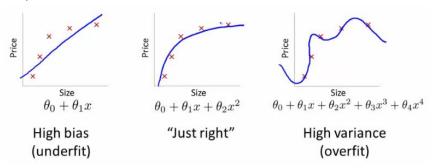
Khi training model thì không phải lúc nào (hàm mất mats) loss của tập train và tập test cũng đồng thời giảm, tới một epoch nào đó thì loss của tập train sẽ tiếp tục giảm nhưng loss của tập test không giảm mà tăng trở lại => Đó là hiện tượng overfitting. Vì vậy để ngăn chặn nó, thì ngay tại thời điểm đó người ta sẽ dừng việc training (vì để chương trình tiếp tục training thì cũng không cải thiện được gì mà lại tốn tài nguyên).

3.2 Underfitting (chưa khớp):

Underfitting (chưa khớp) là hiện tượng khi mô hình xây dựng chưa có độ chính xác cao trong tập dữ liệu huấn luyện cũng như tổng quát hóa với tổng thể dữ liệu. Khi hiện tượng Underfitting xảy ra, mô hình đó sẽ không phải là tốt với bất kì bộ dữ liệu nào trong vấn đề đang nhắc tới.

Phát hiện underfitting

Một cách để phát hiện tình huống như vậy là sử dụng phương pháp tiếp cận phương sai lệch, có thể được biểu diễn như sau:



Mô hình gặp vấn đề underfitting khi nó có bias cao.

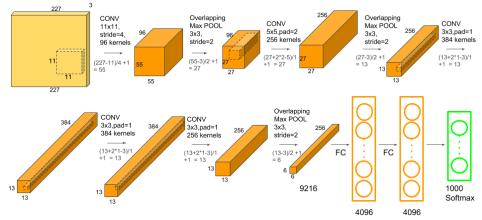
Cách để ngăn chặn vấn đề Underfitting:

Nhiều dữ liệu hơn nói chung sẽ không giúp ích được gì. Trên thực tế, nó có khả năng làm tăng lỗi training. Do đó chúng ta nên tăng thêm nhiều tính năng. Vì điều đó mở rộng không gian giả thuyết. Điều này bao gồm việc tạo ra các tính năng mới từ các tính năng hiện có. Tương tự như vậy, nhiều tham số hơn cũng có thể mở rộng không gian giả thuyết.

4. Model:

Model được nhóm sử dụng là model AlexNet

AlexNet là một mô hình CNN cơ bản, đơn giản và hiệu quả. Trong đó chủ yếu bao gồm các giai đoạn xếp tầng, như là lớp convolution, lớp pooling, lớp rectified linear unit (ReLU) và lớp fully connected như hình bên dưới



Kiến trúc AlexNet

Cấu trúc các lớp

Kiến trúc AlexNet bao gồm 5 lớp convolutional 5 và 3 lớp fully connected. Bên cạnh đó thực hiện ReLu và chuẩn hóa được thực hiện sau mỗi lớp convolutional.

Những convolution layer (hay còn gọi với tên khác là các filter) rút trích các thông tin hữu ích trong các bức ảnh. Trong một convolution layer bất kỳ thường bao gồm nhiều kernel có cùng kích thước. Ví dụ như convolution layer đầu tiên của AlexNet chứa 96 kernel có kích thước 11x11x3. Thông thường thì width và height của một kernel bằng nhau, và độ sâu (depth) thường bằng số lượng kênh màu.

Convolutional 1 và convolution 2 kết nối với nhau qua một Overlapping Max Pooling ở giữa. Tương tự như vậy giữa convolution 2 và convolution 3. Convolutional 3, convolution 4, convolution 5 kết nối trực tiếp với nhau, không thông qua trung gian. Convolutional 5 kết nối fully connected layter 1 thông qua một Overlapping Max pooling, tiếp theo mà một fully connected layter nữa. Và cuối cùng là một bộ phân lớp softmax với 1000 lớp nhãn

Overlapping Max Pooling

Max Pooling layer thường được sử dụng để giảm chiều rộng và chiều dài của một tensor nhưng vẫn giữ nguyên chiều sâu. sử dụng pooling có kích thước 3x3 và bước nhảy là 2 giữa các pooling. Nghĩa là giữa pooling này và pooling khác sẽ overlapping với nhau 1 pixel. Các thí nghiệm thực tế đã chứng minh rằng việc sử dụng overlapping giữa các pooling giúp giảm độ lỗi top-1 error 0.4% và top-5 error là 0.3% khi so với việc sử dụng pooling có kích thước 2x2 và bước nhảy 2 (vector output của cả hai đều có số chiều bằng nhau).

ReLU Nonlinearity

Sử dụng ReLU mô hình deep CNN sẽ huấn luyện nhanh hơn so với việc sử dụng tanh hoặc sigmoid.

Công thức của ReLU là: f(X) = max(0,x)

Normalization

Sau khi sử dụng ReLU, hàm sẽ không có range như hàm tanh và sigmoid, vì vậy nên sử dụng chuẩn hóa.

$$p_{x,y}^i = a_{x,y}^i / \left(k + \alpha \sum_{j=\max(0,i-n/2)}^{\min(N-1,i+n/2)} (a_{x,y}^j)^2\right)^{\beta}$$
Normalization

Dropout

Với gần 60 triệu tham số trong tập huấn luyện, việc overfitting xảy ra là điều dễ hiểu. Để giải quyết thì sử dụng kỹ thuật dropout. Kỹ thuật này khá đơn giản, một neural sẽ có xác suất bị loại khỏi mô hình là 0.5. Khi một neural bị loại khỏi mô hình, nó sẽ không được tham qia vào quá trình lan truyền tiến hoặc lan truyền ngược. Cho nên, mỗi giá trị input sẽ đi qua một kiến trúc mạng khác nhau. Trong quá trình test, toàn bộ network được sử dụng, không có dropout, tuy nhiên, giá trị output sẽ scaled bởi tham số 0.5 tương ứng với những neural không sử dụng trong quá trình trainning. Với việc sử dụng dropout, chúng ta sẽ tăng gấp đôi lần lặp cần thiết để đạt được độ hội tụ, nhưng khi không sử dụng dropout, mạng AlexNet rất dễ bị overfitting.

Vì sao chọn:

Vì mô hình này có độ chính xác khá cao 91.613%

5. Ưu điểm và nhược điểm của model

Advantages

- AlexNet là CNN đầu tiên sử dụng GPU để train, nên nó train rất nhanh.
- Sử dụng ReLU mang tới 2 lợi thế đó là: không giới hạn output như các hàm activation khác, điều này có nghĩa là không có quá nhiều loss function
- Đầu ra không có giá trị âm. Điều này có nghĩa là nó sẽ cải thiện tốc độ train model bởi vì không phải tất cả perceptron đều hoạt động

Disadvantages

- So với các model mới hơn thì, Model này không có hiệu quả bằng bởi vì nó phải học đặc điểm từ các tấm hình.
- Sử dụng nhiều thời gian hơn các model sau này trong việc train để đạt được kết quả accuracy cao hơn

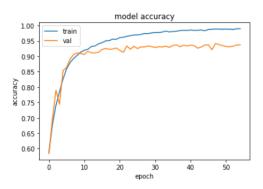
6. Trình bày kết quả nhận được và giải thích

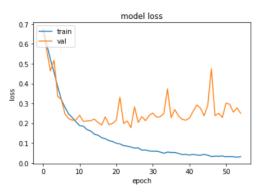
Độ chính xác: 93.375%

Model: "sequential"

Layer (type)	Output S	Shape 	Para	ım #	!
conv1 (Conv2D)	(Non	e, 227, 22	7, 64)	17	92
conv2 (Conv2D)	(Non	e, 55, 55, ⁹	96)	743	520
maxpool1 (MaxPo	ooling2D)	(None, 2	7, 27, 9	5)	0
conv3 (Conv2D)	(Non	e, 27, 27,	256)	614	1656
maxpool2 (MaxPo	ooling2D)	(None, 1	3, 13, 2	56)	0
conv4 (Conv2D)	(Non	e, 13, 13,	384)	885	5120
conv5 (Conv2D)	(Non	e, 13, 13,	384)	132	27488
conv6 (Conv2D)	(Non	e, 13, 13,	256)	884	1992
maxpool3 (MaxPo	ooling2D)	(None, 6	, 6, 256		0
flatten (Flatten)	(None,	9216)	0		
dense (Dense)	(None	, 4096)	377	7528	332
dense_1 (Dense)	(Non	e, 4096)	10	5781	312
dense_2 (Dense)	(Non	e, 1000)	40)970	000
dense_3 (Dense)	(Non	e, 1)	100	1	

Total params: 63,089,713 Trainable params: 63,089,713 Non-trainable params: 0





Đạt được kết quả vậy vì máy đã được train qua 20 epochs và sử dụng nhiều hình ảnh được generate dựa vào các ảnh góc, từ đó máy có nhiều góc nhìn đa dạng để tăng tỉ lệ nhận dạng

7. Idea for improvement:

Cải thiện bằng cách cải thiện hyper-parameter

- Tối ưu Learning Rate (LR) → Giảm dần learing rate sau mỗi epoch
- Batch Size → Dùng max batch size mà GPU có thể xử lí ở bài làm sử dụng batch size = 32
- Tăng độ phức tạp của model → tăng thêm nhiều lớp

Cải thiện bằng cách điều chỉnh lại dữ liệu

- Tăng kích thước của input shape → ở bài bọn em đã tăng từ 128,128,3 lên 227,227,3
- Xoay ảnh ngẫu nhiêu
- Trượt ảnh ngẫu nhiên
- Lật ngang-dọc

Cải thiện bằng cách cải thiện model

- Chỉnh lại model với tập dữ liệu con, bỏ một số mẫu dữ liệu cho một số lớp dữ liệu được lấy mẫu quá mức.
- Train lai model

8. Các file cần thiết:

final model.h5:

https://studenthcmusedu-

my.sharepoint.com/:u:/g/personal/19127525_student_hcmus_edu_vn/EUfrX0QDy7lErWMnXYSKNU8Br mgPLHXxLRQnztb4UJtJgg?e=VeU3mQ

dogs-vs-cats.zip:

https://www.kaggle.com/c/dogs-vs-cats/data

hoặc

https://studenthcmusedu-

my.sharepoint.com/:u:/g/personal/19127525 student hcmus edu vn/EYip60GjDlpOkjaReE33d88BK5TE oVWqem0UydHD3oehhA?e=5rnDCi

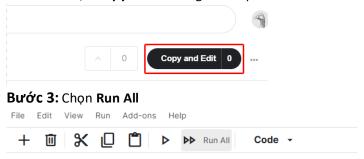
NHÓM 7

9. Hướng dẫn chạy code

Cách 1:

Bước 1: Truy cập đường link: https://www.kaggle.com/tquntv/19127392-19127525-19127625 (Sử dụng trực tiếp project của nhóm bọn em trên kaggle)

Bước 2: Chọn Copy and Edit ở góc bên phải



Cách 2:

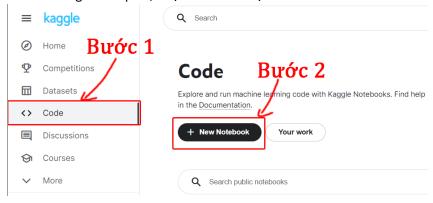
Bước 1: Truy cập trang web: https://www.kaggle.com/#



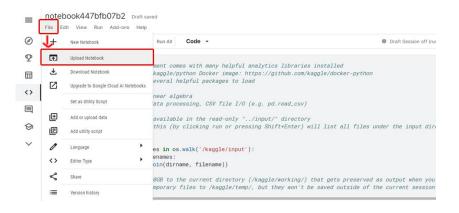
Đăng nhập:

- Nếu không có tài khoản, chọn Register để đăng kí
- Chọn **Sign In** để đăng nhập

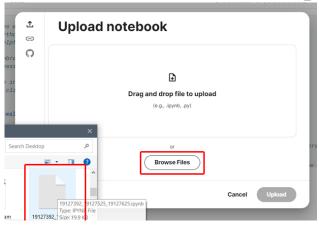
Bước 2: ở góc bên phải, chọn **Code** → chọn **New Notebook**



Bước 3: Chọn File → Upload Notebook



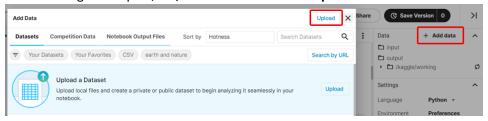
Bước 4: Chọn Browse Files → chọn File 19127392_19127525_19127625.ipynb → Nhấn Upload



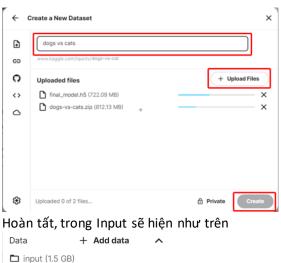
Bước 5: Upoad File

Cách 1:

Bước 1: Ở góc bên phải, chọn + Add data → nhấn Upload

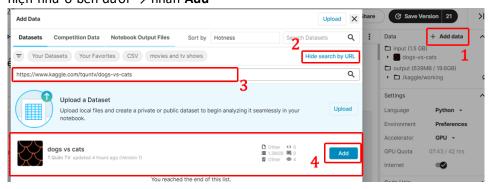


Bước 2: Nhấn **Browse File** \rightarrow chọn 2 file **final_model.h5** và **dogs-vs-cats.zip** \rightarrow đặt tên data set: **dogs vs cats** \rightarrow sau khi 2 file Upload xong \rightarrow nhấn **Create**



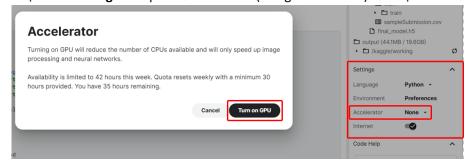
Data	+ Add data	^						
input (1.5 GB)								
▼ dogs-vs-cats								
▶ ☐ dogs-vs-cats								
final	_model.h5							
□ output								
▶ 🗖 /kaggl	e/working	G 5						

Cách 2: Chọn + Add data → Nếu ở ô thứ 2 bên dưới có chữ Hide search by URL → khỏi nhấn, nếu có chữ **Search by URL** \rightarrow nhấn \rightarrow ở ô nhập URL(3) \rightarrow dán vào đường dẫn https://www.kaggle.com/tquntv/dogs-vs-cats → Kaggle se load dataset online của nhóm và hiện như ở bên dưới → nhấn Add



Bước 6: Mở GPU

Chọn Tab **Settings** bên phải → vào **None** (trong Accelerator) → Chọn **GPU** → Chọn **Turn on GPU**



Bước 7: Chọn Run All

NHÓM 7 11



10. Quá trình chạy dữ liệu

Sau khi nhấn Run All, kaggle sẽ tiến hành chạy hết tất cả các Cell

Trước tiên máy sẽ chạy cell **Tạo cây thư mục**

Sau khi chạy xong, cell này sẽ thông báo như này, quá trình chạy có thể kéo dài từ 30 giây đến 1 phút

```
Create subdirectory......Done!
Cat: 12500
Dog: 12500
Classify directory......Done!
```

Tiếp đến chạy cell Data Augment

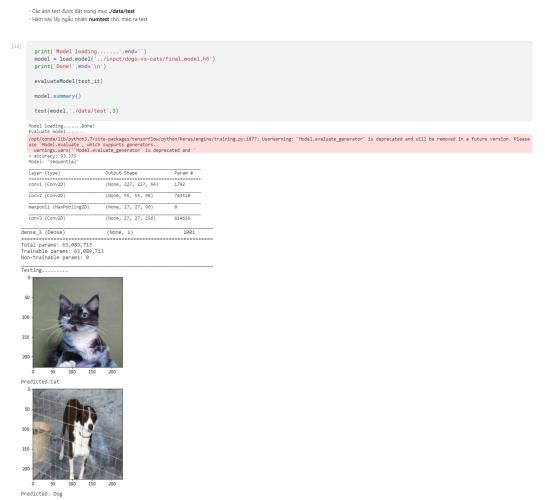
Data Augment

Sử dụng ImageDataGenerator để tạo thêm các ảnh mới từ tập ảnh gốc bằng cách: lật ngang, lật dọc, kéo méo ảnh, phóng to, thu nhỏ ảnh, tăng giảm sáng, tương phân, thêm noise...

— Nhằm đã dạng góc nhìn về các bức ảnh để train model

Chạy cell Load model để nạp model đã train dở (nếu trước có train dở)

Kế đến là cell **(Main) Test model đã train từ trước**, ở đây sẽ tự động nạp model final_model.h5 đã train sẵn từ trước, chạy, hiển thị kết quả và dự đoán 1 số ảnh random trong mục ./data/test (Main) Test model đã train từ trước



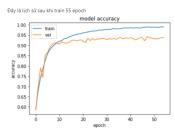
Sau cùng là cell (Main) Train và chạy lại từ đầu, để thầy có thể xem được quá trình train 55 epoch

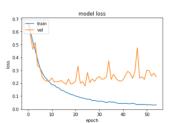
(Main) Train và chạy lại từ đầu

Ở cell cuối cùng, không có chạy code, nó chỉ show biểu đồ quá trình train 55 epoch

```
Epoch 00010: val_accuracy did not improve from 0.90280 [
| Fpoch 11/55 |
| Fpoch 00011: val_accuracy did not improve from 0.90280 [
| Fpoch 00011: val_accuracy did not improve from 0.90280 [
| Fpoch 00011: val_accuracy did not improve from 0.90280 [
| Fpoch 12/55 |
| Fpoch 12/55 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360, saving model to ./checkpoint.h5 [
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360, saving model to ./checkpoint.h5 [
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360, saving model to ./checkpoint.h5 [
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360, saving model to ./checkpoint.h5 [
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360, saving model to ./checkpoint.h5 [
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accuracy improved from 0.90280 to 0.91360 |
| Fpoch 00012: val_accur
```

Kết quả tóm tắt lịch sử train





11. Reference

AlexNet:

https://www.phamduytung.com/blog/2018-06-15-understanding-alexnet/

AlexNet Architecture:

https://www.kaggle.com/blurredmachine/alexnet-architecture-a-complete-guide

Avance + Disavance of AlexNet:

https://tejasmohanayyar.medium.com/a-practical-experiment-for-comparing-lenet-alexnet-vgg-and-resnet-models-with-their-advantages-d932fb7c7d17

Training, Test, Validate:

https://www.mrtech.vn/2018/11/training-set-testing-set-validation-set.html

Overfitting, Underfitting:

https://cuonglv1109.blogspot.com/2018/11/overfitting-la-gi.html https://khanh-personal.gitbook.io/ml-book-vn/chapter1/overfitting https://viblo.asia/p/cac-phuong-phap-tranh-overfitting-gDVK24AmlLi

Improve performance:

https://towardsdatascience.com/the-quest-of-higher-accuracy-for-cnn-models-42df5d731faf

Classification using AlexNet:

 $\underline{https://vitorgabo.medium.com/cats-and-dogs-classification-using-alexnet-5fc52b1cc1a6}$

Call back:

https://miai.vn/2020/09/05/keras-callbacks-tro-thu-dac-luc-khi-train-models/

Save và load model:

https://tek4.vn/cach-luu-va-load-lai-mot-mo-hinh-hoc-sau-keras-co-ban