TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG



BÁO CÁO **MÔN HỌC**

Học máy

Đề tài: So sánh thử nghiệm các phương pháp học máy cho bài toán phân loại ảnh.

Nhóm sinh viên thực hiện:

Họ và tên	MSSV	Lớp
Nguyễn Tuấn Đạt	20130856	CNTT2.02-K58
Vũ Minh Đức	20130856	CNTT2.02-K58
Nguyễn Ngọc Huyền	20130856	CNTT2.02-K58
Đặng Quang Trung	20130856	CNTT2.02-K58
Phan Anh Tú	20130856	CNTT2.02-K58

Giáo viên hướng dẫn: TS.Thân Quang Khoát

Mục lục

Là	i cám ơn	3
Da	nh sách hình vẽ	4
1	Mở đầu	5
2	Giới thiệu bài toán 2.1 Giới thiệu bài toán	6
3	Các phương pháp sử dụng và kết quả thực nghiệm 3.1 KNN 3.1.1 Cơ sở lý thuyết 3.1.2 Cài đặt 3.1.3 Kết quả 3.2 Mạng neural 3.2.1 Cơ sở lý thuyết 3.2.2 Cài đặt	77 77 78 89 99
	3.2.3 Kết quả Convolutional Neural Networks(CNN) 3.3.1 Giới thiệu 3.3.2 Kiến trúc tổng quan CNN 3.3.3 Update tham số 3.3.4 Mạng CNN Đơn giản 3.3.5 Mạng CNN Lớn 3.4.1 Cơ sở lý thuyết SVM 3.4.2 Cơ sở lý thuyết 3.4.3 Cài đặt áp dụng với bài toán phân loại ảnh 3.4.4 Kết quả thực nghiệm	9 9 11 12 14 15 16 18
4	Kết luận 4.1 So sánh các phương pháp	20 20 20 20
5	Tài liêu tham khảo	21

Lời cảm ơn

Danh sách hình vẽ

3.1	Function distance KNN	8
3.2	Split data	8
3.3	Histogram	16
3.4	Siêu phẳng phân tách	16

Phần 1 Mở đầu

Phần 2

Giới thiệu bài toán

- 2.1 Giới thiệu bài toán
- 2.2 Bộ dữ liệu sử dụng

Phần 3

Các phương pháp sử dụng và kết quả thực nghiệm

3.1 KNN

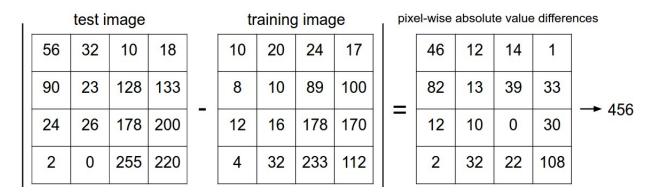
3.1.1 Cơ sở lý thuyết

- Giai đoạn học
 - KNN K nearest neighbors : là một phương pháp học máy dựa trên việc lưu lại các các ví dụ học trong tập dữ liệu training.
- Giai đoạn phân lớp
 - Dùng một hàm để tính độ tương đồng giữa các ví dụ traning đã lưu và dữ liệu từ bộ test.
 - Lưu lại k ví dụ có độ tương đồng với dữ liệu test nhất, từ đó dự đoán nhãn cho ví dụ test đầu vào theo lớp chiếm số đông trong số các lớp của k láng giềng.
- Vấn đề cần giải quyết với giải thuật KNN
 - Có nhiều hàm tính độ tương đồng, cần lựa chọn và thử nghiệm để chon ra hàm tương đồng phù hợp với bộ dữ liệu.
 - Lấy bao nhiêu hàng xóm cho đủ.

3.1.2 Cài đặt

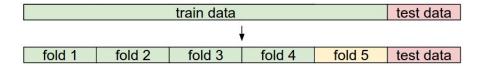
- Biểu diễn dữ liệu: mỗi dữ liệu sẽ được biểu diễn thông qua các vector $x = (x_1, x_2, ..., x_n, y)$
 - $-x_i$ là các thuộc tính
 - y là nhãn lớp
- Lựa chọn mô hình

– Hàm tính độ tương đồng :D(x,y)= $\sum_{i=1}^{n} (\|x_i - y_i\|)$



Hình 3.1: Function distance KNN

– Lựa chọn k:



Hình 3.2: Split data

- * Bước đầu, dữ liệu được chia ra thành 2 phần train và test
- * Tiếp theo từ tập train, chia dữ thành 5 fold, lấy 4 fold cho việc học, 1 fold dùng validation
- $\ast\,$ Thử cho các giá trị k=3,4,5,6,7, lựa chọn các giá trị tốt nhất

(ghi chú: cần nêu rõ cấu trúc mã nguồn, chương trình, vai trò của các lớp và các phương thức chính)

3.1.3 Kết quả

- \bullet K thu được là 7
- Kết quả $\approx 11\%$

Bảng 3.1: **Bảng mô tả kết quả KNN**

0	1	2	3	4	5	6	7	8	9
40%	2%	13.6%	1.2%	23.3%	1.5%	1.3%	1.1%	14.6%	1%
38%	5%	13%	2%	24%	1%	2.2%	1.1%	12%	1.5%
48%	1.4%	17%	0.5%	13%	0.2%	0.5%	1.6%	17%	0.8%
45%	2.3%	12%	2%	18%	0.8%	0.5%	3.1%	12%	4.2%
60%	4.4%	10%	2.5%	8%	1.2%	3.5%	0.1%	10%	0.2%
54%	1.4%	18%	0.5%	11%	4.1%	0.5%	0.9%	18%	0.6%
50.1%	0.1%	12.5%	1.1%	17%	0.2%	0.5%	0.2%	17%	0.2%

48%	0%	15.7%	0%	0%	0%	0%	0%	18.6%	0%
35.3%	4.4%	12.3%	0.6%	17.9%	1.9%	0.1%	0%	27.3%	0.2%
45.8%	1%	14.7%	2.3%	19.2%	1%	0.3%	0%	15.5%	0.2%

3.2 Mang neural

- 3.2.1 Cơ sở lý thuyết
- 3.2.2 Cài đặt
- 3.2.3 Kết quả

3.3 Convolutional Neural Networks(CNN)

3.3.1 Giới thiệu

Convolutional Neural Networks tương tư như các mạng nerual network khác. Chúng được tạo thành từ các tế bào noron có thể học trọng số và biases. Mỗi noron thực hiện hiện một số sản xuất và tùy chọn với đường phi tuyến. Toàn bộ mạng vẫn thể hiện một hàm số khả vi duy nhất: từ các điểm ảnh hình ảnh thô trên một đầu với điểm số lớp học khác. Chúng vẫn có một hàm lỗi (ví dụ như SVM/softmax) ở lớp cuỗi (với kết nối đầy đủ).

3.3.2 Kiến trúc tổng quan CNN

Mạng CNN có 4 tầng chính: Convolution Layer, ReLu Layer , Pooling Layer, Fully-Connected Layer.

Lớp Convolution Layer (Conv)

- Nhận đầu vào là ma trận các điểm ảnh $(W_1 * H_1 * D_1)$ $(W_1 * H_1$: kích thước của ảnh, D_1 số kênh màu (3 kênh màu nếu là ảnh màu đại diện cho 3 kênh màu (r,g,b))).
- Các tham số:
 - Số các filters K: Tham số chính của tâng Conv. Mỗi filter sẽ trượt qua ma trận đầu vào và đưa ra ma trận đầu ra. Mỗi filter là một ma trận có kích thước là tham số cần chọn, chiều của ma trận là chiều của ma trận đầu vào (trong bài toán này chiều của filter là 3 (số kênh màu)).
 - Kích thước của mỗi filter F*F.
 - Số ô nhat qua mỗi lần trượt.

- Zerro padding P: Tham số quyết định ma trận đầu vào và ma trận đầu ra có cùng kích thước không (có trượt hết tất cả các ô của ma trận đầu vào không hay nói cách khác là có trượt vượt ra khỏi ma trận đầu vào không).
- Đầu ra là ma trận kích thước $W_2 * H_2 * D_2$:
 - $W_2 = (W_1 F + 2P)/S + 1$.
 - $H_2 = (H_1 F + 2P)/S + 1$.
 - $D_2 = K$.

Lớp RELU Layer

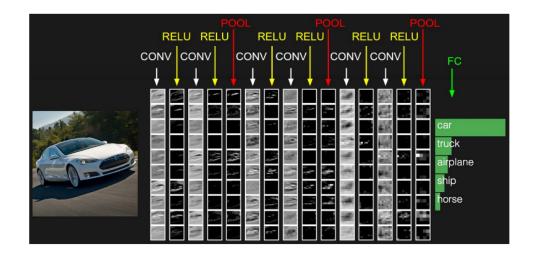
Tầng sẽ áp dụng hàm tác động, thông thường sẽ làm hàm ReLu $\max(0,x)$. Hàm sẽ tác động lên từng phần tử của ma trận đầu vào nên ma trận đi qua tầng này sẽ không thay đổi kích thước.

Lớp PoolingLayer

- Thường chèn tầng pooling vào giữa các tầng Conv để giảm kích thước ma trận.
- Nhận đầu vào là ma trận $W_1 * H_1 * D_1$ là kích thước của ma trận đầu ra của tầng Conv.
- Các tham số:
 - Kích thước của ma trận pooling F * F.
 - Số ô nhảy qua sau mỗi lần trượt trên ma trận input.
- Đầu ra là mậ trận kích thước $W_2 * H_2 * D_1$.
 - $W_2 = \frac{(W_1 F)}{S} + 1$.
 - $H_2 = \frac{(H_1 F)}{S} + 1$.
 - $D_2 = D_1$.

Lớp Fully-connected Layer

- Như mạng neuron thông thường,các neuron trong tầng Fully-connected kết nối với toàn bộ các neuron ở tầng trước nó: Nhận đầu vào là vector áp dụng hàm tác động và đưa ra đầu ra.



Lớp Max norm constraint và Dropout

Để giảm overfit ta có thể áp dụng các kỹ thuật như:

- Thêm max norm constraint cho các trọng số.
 - Khi cập nhật các trọng số thì các trường số phải thỏa mãn điều kiện: $\|\overrightarrow{w}\|_2 < c(c)$ thường được chọn 3 hoặc 4).
- Thêm tầng dropout
 - Đầu ra của các tầng trước tầng drop-out khi đi qua tầng drop-out sẽ được giữ nguyên với xác là p hoặc sẽ được chuyển thành 0 với xác suất 1-p.

3.3.3 Update tham số

Momentum update

$$\Delta w^{t+1} = \Delta w^t + \mu.\Delta w^t - \eta.\nabla E^t.$$

Nesterov momentum

$$w^{(t+1)=w^t+\mu.\Delta w^t} \\ \Delta w^{(t+1)} = \mu.\Delta w^t - \eta.\nabla E^{t+1}.$$





3.3.4 Mạng CNN Đơn giản

Cấu trúc mạng

Cài đặt chương trình

Sử dụng thư viện keras

- Load data và xử lí dữ liệu:

```
(X_train, y_train), (X_test, y_test) = cifar10.load_data()
# normalize inputs from 0-255 to 0.0-1.0

X_train = X_train.astype('float32')

X_test = X_test.astype('float32')

X_train = X_train / 255.0

X_test = X_test / 255.0

# one hot encode outputs

y_train = np_utils.to_categorical(y_train)

y_test = np_utils.to_categorical(y_test)

num_classes = y_test.shape[1]
```

- Thêm các tầng

```
model.add(Convolution2D(32, 3, 3, input_shape=(3, 32, 32), border_mode='same', activation='relu', W_constraint=maxnorm(3)))

model.add(Dropout(0.2))

model.add(Convolution2D(32, 3, 3, activation='relu', border_mode='same', W_constraint=maxnorm(3)))

model.add(MaxPooling2D(pool_size=(2, 2)))

model.add(Flatten())

model.add(Dense(512, activation='relu', W_constraint=maxnorm(3)))

model.add(Dropout(0.5))

model.add(Dense(num_classes, activation='softmax'))
```

- Các tầng Conv có các tham số:
 - * Số filter: 32
 - * Kích thước mỗi filter: 3 * 3 * 3.
 - * input_shape: Nhận đầu vào là ma trận ảnh 32 * 32 * 3.
 - * border_mode: kích thước ma trận đầu vào và ma trận đầu ra là như nhau (32*32).

- * W constraint: max norm constraint với c = 3.
- Sau mỗi tầng Conv là tầng ReLu
- \bullet Tầng Drop-out thứ nhất với xác suất chuyển các tham số về 0 là 0.2
- Tầng Pooling với fiter có kích thước 2*2
- Tầng Flattern để chuyển ma trận thành vector
- Tầng Dense (Fully-connected):
 - * Kích thước đầu ra: 512 (vector 512 chiều)
 - * Hàm tác động: relu
 - * W_constraint: max norm constraint với c = 3
- \bullet Tầng Drop-out thứ hai với xác suất chuyển các tham số về 0 là 0.2
- Tầng Dense (Fully-connected) cuối cùng:
 - * Kích thước đầu ra: Số nhãn lớp (scroce cho mỗi nhàn lớp): 10 nhãn lớp
 - * Hàm tác động : softmax (vector x có n chiều)

$$\sigma(x_i) = \frac{e^{x_i}}{\sum_{j=1}^n e^{x_k}}$$

- Traning:

```
epochs = 25

Irate = 0.01

decay = Irate/epochs

sgd = SGD(Ir=irate, momentum=0.9, decay=decay, nesterov=False)

model.compile(loss='categorical_crossentropy', optimizer=sgd, metrics=['accuracy'])

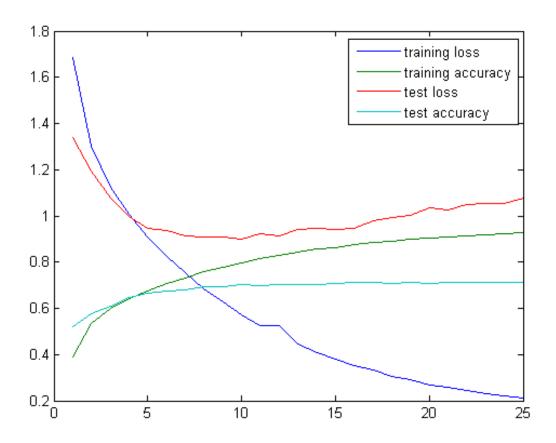
print(model.summary())

# Fit the model

model.fit(X_train, y_train, validation_data=(X_test, y_test), nb_epoch=epochs, batch_size=32)
```

- Số epoch thực hiện 25
- Learning rate: 0.01
- Sử dụng minibatch gradient decent (số ảnh trong một batch là 32) với chiến lược tối ưu là momentum để update các tham số (tham số mu trong momentum là 0.9) không sử dụng nesterov momentum
- Hàm đánh giá lỗi: cross-entropy

 $L = -\frac{1}{N} \sum_{i=1}^{N} [y_i \log y_i + (1 - \tilde{y}_i)] \text{ (c là nhãn thực tế của ảnh i}, \tilde{y}_i \text{ là nhãn do mô hình dự đoán)}$



Kết quả

3.3.5 Mạng CNN Lớn

Cấu trúc mạng

 $\begin{array}{lll} INPUT \ \rightarrow \ CONV \ \rightarrow \ RELU \ \rightarrow \ DropOut \ \rightarrow \ [CONV \ \rightarrow \ RELU \ \rightarrow \ POOL] *2 \ \rightarrow \\ DropOut \ \rightarrow \ CONV \ \rightarrow \ RELU \ \rightarrow \ POOL \ \rightarrow \ FLatten[DropOut \ \rightarrow \ Fully-connect(RELU)] *2 \ \rightarrow \\ DropOut \ \rightarrow \ Ouput(num \ class, activation='s oftmax') \end{array}$

Bảng 3.2: **Bảng mô tả mạng CNN**

Layer (type)	Output Shape	Param#	Connected to
convolution2d_1 (Convolution2D)	(None, 32, 32, 32)	896	${\rm convolution2d_input_1[0][0]}$
dropout_1 (Dropout)	(None, 32, 32, 32)	0	$convolution 2d_1[0][0]$
convolution2d_2 (Convolution2D)	(None, 32, 32, 32)	9248	$dropout_1[0][0]$
maxpooling2d_1 (MaxPooling2D)	(None, 32, 16, 16)	0	$convolution 2d_2[0][0]$
convolution2d_3 (Convolution2D)	(None, 64, 16, 16)	18496	$maxpooling2d_1[0][0]$
maxpooling2d_2 (MaxPooling2D)	(None, 64, 8, 8)	0	$convolution 2d_3[0][0]$
convolution2d_4 (Convolution2D)	(None, 128, 8, 8)	73856	$maxpooling2d_2[0][0]$
dropout_2 (Dropout)	(None, 128, 8, 8)	0	$convolution 2d_4[0][0]$
convolution2d_5 (Convolution2D)	(None, 128, 8, 8)	147584	$dropout_2[0][0]$
maxpooling2d_3 (MaxPooling2D)	(None, 128, 4, 4)	0	${\rm convolution2d_5[0][0]}$
flatten_1 (Flatten)	(None, 2048)	0	$maxpooling2d_3[0][0]$
dropout_3 (Dropout)	(None, 2048)	0	$flatten_1[0][0]$
dense_1 (Dense)	(None, 1024)	2098176	$dropout_3[0][0]$
dropout_4 (Dropout)	(None, 1024)	0	$dense_1[0][0]$
dense_2 (Dense)	(None, 512)	524800	$dropout_4[0][0]$
dropout_5 (Dropout)	(None, 512)	0	$dense_2[0][0]$
dense_3 (Dense)	(None, 10)	5130	$dropout_5[0][0]$

Tổng params: 2878186

3.4 SVM

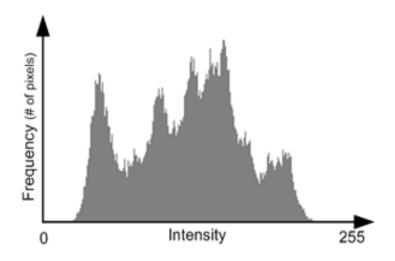
3.4.1 Cơ sở lý thuyết SVM

Khái niệm-đặc điểm

SVM là một phương pháp phân lớp tuyến tính (linear classifier), với mục đích xác định một siêu phẳng (hyperplane) để phân tách hai lớp của dữ liệu. SVM có một nền tảng lý thuyết chặt chẽ

SVM là một phương pháp tốt (phù hợp) đối với những bài toán phân lớp có không gian rất nhiều chiều (các đối tượng cần phân lớp được biểu diễn bởi một tập rất lớn các thuộc tính)

Biểu đồ histogram: Histogram là một dạng biểu đồ biểu diễn số lượng điểm ảnh tương ứng với mức độ sáng tối của bức ảnh.



Hình 3.3: Histogram

3.4.2 Cơ sở lý thuyết

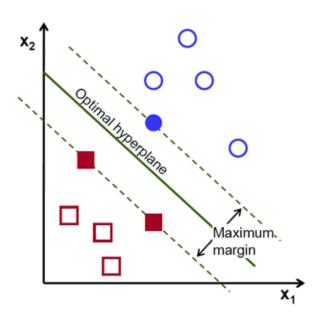
Biểu diễn tập huấn luyện

$$x_1, y_1, (x_2, y_2), ...(x_r, y_r)$$

- $\bullet \ x_i$ là một vectơ đầu vào $x_i \subseteq R^n$
- $\bullet \ y_i \in {1,-1}$ là một nhãn lớp Hàm phân tách tuyến tính

$$f(x) = \langle w.x \rangle + b$$

w là vectơ trọng số các thuộc tính, b là một giá trị số thực



Hình 3.4: Siêu phẳng phân tách

Khoảng cách từ một điểm đến siêu phẳng

$$\frac{|< w.x_i > +b|}{||w||}$$

$$margin = d_{+} + d_{-} = \frac{2}{||w||}$$

Tương đương bài toán cực tiểu hóa $\frac{< w.w>}{2}$ với điều kiện

$$\{ \begin{array}{l} < w.x_i > +b \ge 1 \\ < w.x_i > +b \le -1 \\ if y_i = -1 \end{array}$$

Áp dụng phương pháp Lagrange

$$L = 1/2||\overline{w}||^2 - \sum \alpha_i [y_i(\overline{w}.\overline{x_i} + b) - 1]$$

Điều kiện

$$\frac{\partial}{\partial \overline{w}} = \overline{w} - \sum \alpha_i y_i x_i = 0 \Longrightarrow \overline{w} = \sum \alpha_i y_i \overline{x_i}$$
$$\frac{\partial}{\partial b} = -\sum \alpha_i y_i \Longrightarrow \sum x_i y_i = 0$$

Thế vào ta được biểu thức:

$$L_D(\alpha) = \sum_{i=1}^r \alpha_i - 1/2 \sum_{i,j=1}^r \alpha_i \alpha_j y_i y_j < x_i \cdot x_j >$$

Điều kiện:

$$\begin{cases} \sum_{i=1}^{r} \alpha_i y_i = 0\\ \alpha_i \ge 0 \forall i = 1..r \end{cases}$$

Dung phương pháp lặp giải cuối cùng thu được

$$w^* = \sum_{x_i \in SV} \alpha_i y_i x_i$$

$$b^* = y_k - \langle w^*, x_k \rangle$$

Để phân lớp cho giá trị mới ta tìm dấu của siêu phẳng

$$f(x) = \sum_{x_i \in SV} \alpha_i y_i < x_i \cdot x > +b^*$$

Nới lỏng điểu kiện:

$$L_D(\alpha) = \sum_{i=1}^r \alpha_i - 1/2 \sum_{i,j=1}^r \alpha_i \alpha_j y_i y_j < x_i \cdot x_j >$$

$$\begin{cases} \sum_{i=1}^r \alpha_i y_i = 0\\ 0 \le \alpha_i \le C \forall i = 1..r \end{cases}$$

Phân lớp không tuyến tính một vài hàm nhân: Đa thức $K(x,z)=(< x.z>+\Theta)^d$ Gaussian RBF $K(x,z)=e^{\frac{||x-z||^2}{2*\sigma}}$ trong đó $\sigma>0$ Phân lớp nhiều nhãn 2 chiến lược :

- one-versus-rest
- one-versus-one

3.4.3 Cài đặt áp dụng với bài toán phân loại ảnh

Công cụ

Ngôn ngữ lập trình python, thư viện học máy scikit-learn, opency Đọc dữ liệu :

```
#have 5 bacth
#read batch 1
fo = open("data_batch_1", 'rb')
dict = cPickle.load(fo)
da=np.array(dict.get('data'))
lb=np.array(dict.get('labels'))
fo.close()
```

Huấn luyện mô hình kernel là hàm nhân sử dụng (rbf,linear,poly) C là tham số nới lỏng mô hình, gamma tham số ảnh của hàm nhân(ảnh hưởng đến giá trị). Với hàm poly ta còn có tham số degree(mũ) và coef0(b) phương thức fit của SVC dùng để train mô hình

```
clf = SVC(C=5, kernel='rbf',gamma='auto')
from datetime import datetime
print("start",str(datetime.now()))
clf.fit(trainX, trainY)
print("end train",str(datetime.now()))
```

Đoán tập test: phương thức predict dùng để đoán nhãn cho tập test

```
res=clf.predict(testX)
print("end predict ",str(datetime.now()))
sol=(res==testY)
print(res[:10])
print(testY[:10])
print(sol[:10])
print(sol.sum())
```

Sử dụng histogram để xây dựng đầu vào cho SVM :

Histogram với rbg color: sử dụng cv2 để tạo ra ma trận histogram , cv nhận đầu vào là ảnh nên ta phải chuyển ma trận từ dữ liệu thành ma trận ảnh rbg kích thước 32 32 3.

Các tham số của hàm calcHist như sau

- Đầu vào ảnh
- \bullet Số đại diện cho màu cần tạo histogram [0 1 2] tức là cả 3 màu r b g
- bin tương ứng từng màu với dữ liệu ảnh theo (1) khuyên nên chọn 16
- Vùng màu chọn

```
histr = cv2.calcHist(da[i].reshape((3,1024)).T.reshape((32,32,3))
lhistr.append(histr.ravel())
trainX=np.array(lhistr)
```

Histogram với gray color: Sử dụng hàm chuyển đổi màu của opency cyt-Color() việc này đồng nghĩa sẽ giảm số chiều của dữ liệu xuống bằng bins ở đây là 16.

```
lhistr=[]
for i in range(50000):
    #print i
    histr = cv2.calcHist(cv2.cvtColor(da[i].reshape((3,1024)).T.reshallhistr.append(histr.ravel())

trainX=np.array(lhistr)
```

Phương pháp đánh giá sử dụng: hold on

3.4.4 Kết quả thực nghiệm

Áp dụng toàn bộ với chiền lược one vs all

- SVM rbf C=5 autosklearn=(gamma=1/3072(xích ma=3072)) độ chính xác $\approx 25\%$
- SVM linear C=5 độ chính xác $\approx 32\%$
- SVM poly histogram bin=16 C=5 autosklearn=(gamma=1/3072 n=3) độ chính xác $\approx 37,6\%$
- SVM poly gray histogram bin=16 C=5 autosklearn=(gamma=1/3072 n=3) độ chính xác $\approx 29,6\%$

Phần 4

Kết luận

4.1 So sánh các phương pháp

4.2 Khó khăn gặp phải

Phương pháp SVM

- \bullet Bộ dữ liệu lớn train rất lâu poly (5 tiếng) r
bf(10 tiếng) rất khó để xử lý chọn các tham số
- SVM rất nhiều tham số cần phải thử nghiệm rất nhiều

4.3 Kinh nghiệm rút ra được

Phần 5

Tài liệu tham khảo

- [+] Slide Học Máy TS. Thân Quang Khoát
- [+] Opencourse in Mit-SVM
- [+] http://www.svm-tutorial.com/2016/09/unconstrained-minimization/
- [+] https://ongxuanhong.wordpress.com/2015/09/19/support-vector-machine
- [+] http://scikit-learn.org/stable/modules/generated/sklearn.svm.SVC.html
- [+] SVMs for Histogram-Based Image Classification
- Olivier Chapelle, Patrick Haffner and Vladimir Vapnik
- [+] http://docs.opencv.org/3.1.0/d1/db7/tutorial_py_histogram_begins.html