به نام خدا



درس یادگیری عمیق

تمرین سری سوم

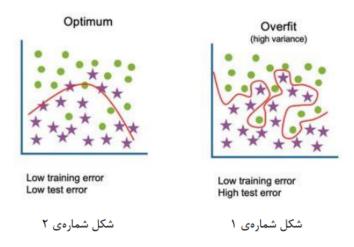
مدرس درس: سرکار خانم دکتر داوودآبادی

تهیه شده توسط: الناز رضایی ۹۸۴۱۱۳۸۷

تاریخ ارسال: ۱۴۰۱/۰۹/۰۹

سوال ١:

- الف) مفهوم overfit در شبکههای عصبی را توضیح دهید. چه موقع گوییم شبکهی عصبی overfit شده است؟ راهکارهای خود برای جلوگیری و حل overfit شدن شبکههای عصبی را نام ببرید. (۱۵ نمره)
- ب) شکل شماره ی ۱ نمایانگر مدل overfit شده بر روی مجموعه ی داده است و شکل شماره ی ۲ مدل normal را نشان میدهد. چرا در شکل شماره ی ۱ مدل برای داده هایی که تاکنون ندیده است، خطای بیشتری نسبت به مدل شکل شماره ۲ تولید خواهد کرد؟ (۱۰ نمره)

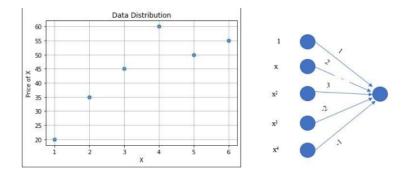


پاسخ ١:

- الف) overfitting به حالتی گفته می شود که مدل ما روی داده های a voverfitting به حالتی گفته می شود که مدل ما روی داده های عملکرد خوبی دارد. در این حالت مدل ما روی داده های دارد اما روی داده های جدید (test) عملکرد ضعیفی دارد. در این حالت مدل ما روی داده های در تنیات آن را یاد گرفته است و حتی ممکن است خطا روی داده های منی شود. از راه حل های جلوگیری از overfitting می توان به کاهش ابعاد شبکه، ارزیابی مدل های یادگیری ماشین، منظم سازی (L_2 و L_1)، داده افزایی (استفاده از برخی تبدیل های ریاضی مانند flip، افزودن نویز، Dropout) اشاره کرد.
- ب) در شکل ۱ مدل روی دادههای overfit ، train شده است و بر روی جزوئیات دادههای

train داده های test، عملکرد ضعیفی خواهد داشت؛ اما شکل شماره ۲، مدل هم روی داده های داده های داده فعیفی خواهد داشت؛ اما شکل شماره ۲، مدل هم روی داده های train عملکرد نسبتا خوبی دارد و همچنین روی داده test عملکرد بهتری نسبت به مدل شماره ۱ دارد. چرا که قابلیت تعمیم دهی آن بیشتر است. در مورد شکل ۱، اتفاقی که میافتد به این صورت است که پس از چند تکرار، بهبود تعمیم دهی متوقف می شود و سپس شروع به تنزل می کند و مدل overfit می شود و الگوهایی را می آموزد که مخصوص داده های آموزشی است اما ارتباط درستی با مسئله مورد نظر ندارد و گمراه کننده است. این موضوع باعث عملکرد ضعیف آن روی داده های test می شود.

سوال ٢:



در این شبکه تابع فعالساز خطی (linear) و نرخ یادگیری ۰.۱ است. تابع خطا را از نوع MSE به فرمول زیر در نظر بگیرید:

$$loss = \frac{1}{2m} \sum_{i=1}^{m} (y - \hat{y})^2$$

• ب) با تغییر مقدار λ چه تغییراتی در میزان خطای تولید شده و نحوه ی آموزش پارامترهای شبکههای عصبی به وجود خواهد آمد $\{1.0, 1.0\}$

پاسخ ۲:

• الف)

- Forward pass:

$$z = w_1 i_1 + w_2 i_2 + w_3 i_3 + w_4 i_4 + w_5 i_5$$

$$\hat{y} = z$$

$$L(y, z) = (y - z)^2 + \frac{\lambda}{2} (\sum_{i=1}^{5} w_i^2)$$

- Backward pass:

$$\begin{split} \frac{\partial L}{\partial z} &= -2(y-z) \\ \frac{\partial L}{\partial w_1} &= \frac{\partial L}{\partial z} \cdot \frac{\partial z}{\partial w_1} = -2i_1(y-z) \\ \frac{\partial L}{\partial w_2} &= \frac{\partial L}{\partial z} \cdot \frac{\partial z}{\partial w_2} = -2i_2(y-z) \\ \frac{\partial L}{\partial w_3} &= \frac{\partial L}{\partial z} \cdot \frac{\partial z}{\partial w_3} = -2i_3(y-z) \\ \frac{\partial L}{\partial w_4} &= \frac{\partial L}{\partial z} \cdot \frac{\partial z}{\partial w_4} = -2i_4(y-z) \\ \frac{\partial L}{\partial w_5} &= \frac{\partial L}{\partial z} \cdot \frac{\partial z}{\partial w_5} = -2i_5(y-z) \end{split}$$

- Update parameters with GD:

$$w_1 = (1 - \eta \lambda)w_1 - \eta \frac{\partial L}{\partial w_1}$$

$$w_2 = (1 - \eta \lambda)w_2 - \eta \frac{\partial L}{\partial w_2}$$

$$w_3 = (1 - \eta \lambda)w_3 - \eta \frac{\partial L}{\partial w_3}$$

$$w_4 = (1 - \eta \lambda)w_4 - \eta \frac{\partial L}{\partial w_4}$$

$$w_5 = (1 - \eta \lambda)w_5 - \eta \frac{\partial L}{\partial w_5}$$

Data 1 (x=1, y=20):

- Forward pass:

$$z = (1*1) + (2*1) + (3*(1)^{2}) + (-2*(1)^{3}) + (-1*(1)^{4}) = 3$$

$$\hat{y} = 3$$

$$L(y, z) = (20-3)^{2} + \frac{0.9}{2}((1)^{2} + (2)^{2} + (3)^{2} + (-2)^{2} + (-1)^{2}) = 297.55$$

- Backward pass:

$$\frac{\partial L}{\partial z} = -2(20 - 3) = -34$$

$$\frac{\partial L}{\partial w_1} = -2(1)(20 - 3) = -34$$

$$\frac{\partial L}{\partial w_2} = -2(1)(20 - 3) = -34$$

$$\frac{\partial L}{\partial w_3} = -2(1)^2(20 - 3) = -34$$

$$\frac{\partial L}{\partial w_4} = -2(1)^3(20 - 3) = -34$$

$$\frac{\partial L}{\partial w_5} = -2(1)^4(20 - 3) = -34$$

- Update parameters with GD:

$$w_1 = (1 - (0.1 * 0.9))1 - 0.1(-34) = 4.31$$

$$w_2 = (1 - (0.1 * 0.9))2 - 0.1(-34) = 5.22$$

$$w_3 = (1 - (0.1 * 0.9))3 - 0.1(-34) = 6.13$$

$$w_4 = (1 - (0.1 * 0.9))(-2) - 0.1(-34) = 1.58$$

$$w_5 = (1 - (0.1 * 0.9))(-1) - 0.1(-34) = 2.49$$

بنابراین، با توجه به محاسبات بالا، وزنهای نهایی شبکه به حالت زیر درمی آیند:

 $w_1 = 4.31$

 $w_2 = 5.22$

 $w_3 = 6.13$

 $w_4 = 1.58$

 $w_5 = 2.49$

 \bullet ب) طبق فرمول، هر چه مقدار λ بیشتر باشد، میزان خطا بیشتر افزایش پیدا میکند و وزنها

به مقدار بیشتری تغییر میکنند؛ اما اگر λ کوچکتر باشد، میزان خظا کمتر افزایش پیدا کرده و وزنها با نرخ کمتری تغییر میکنند.

همچنین افزایش λ ممکن است واریانس بالا (نشانهای از overfitting) را با تشویق وزنهای کوچکتر برطرف کند، که منجر به یک نمودار مرزی تصمیم گیری می شود که با انحنای کمتر ظاهر می شود. به طور مشابه، کاهش λ ممکن است با تشویق وزنهای بزرگتر، بایاس بالا (نشانهای از underfitting) را برطرف کند، که به طور بالقوه منجر به مرز تصمیم گیری پیچیده تر می شود.

سوال ٣:

- الف) یکی از راه کارهای برای متعادل سازی پیچیدگی میان مدل و داده ها برای حالتی که مدل پیچیده تر از داده ها است، افزایش داده های آموزشی است. با این کار به مدل این فرصت داده می شود تا با دیدن حاالت مختلف داده های آموزشی بتواند تعمیم پذیری بیشتری داشته باشد و در نتیجه بهتر آموزش ببیند. اما این راهکار دارای چالش هایی است. یکی از چالش های اساسی این است که توزیع داده ها به هم نخورد هم چنین، تعداد کمی دادة بر چسبدار دررابطه با بسیاری از مسائل وجود دارند که باعث می شود فرایند افزایش تعداد داده های آموزشی، فرایندی بسیار هزینه بر هم از نظر زمانی و هم از نظر مالی باشد. راهکارهای Data Aug.ipynb برای حل این مشکل در افزایش داده ها با هزینة کمتر ارائه شدند. ما در data augmentation و است که برای مجموعة تصاویر داده شده، عملیات Data Aug.ipynb را انجام دهیم و سپس نتیجة آن را ببینیم. برای این کار ابتدا یک مدل MLP داده شده است که باید بر روی مجموعة دادة جدید دوباره از اول آموزش دهید. برای انجام این تمرین مراحل موجود در روی مجموعة دادة جدید دوباره از اول آموزش دهید. برای انجام این تمرین مراحل موجود در این دو آموزش مدل یکسان با مجموعه داده های متفاوت را بنویسید. دربارة overfit نشدن مدل ها صحبت کنید. دلیل خود از استدلال هایتان را نیز بیاورید. (۲۵ نمره) نشدن مدل ها صحبت کنید. دلیل خود از استدلال هایتان را نیز بیاورید. (۲۵ نمره)
- ب) (امتیازی) با استفاده از کتابخانة keras مراحل مربوط به data augmentation را انجام دهید و مجموعة دادة تولید شدة خود را با مجموعة دادة قبلی مقایسه کنید. (۱۵ نمره)

پاسخ ۳:

• الف) در ابتدا، فایل zip داده شده را با دستور "<mzip <path>" از حالت فشرده خارج میکنیم. سپس تصاویر را از directory خوانده و در یک لیست آنها را ذخیره میکنیم. همچنین برای تعیین کلاس آنها، به تصاویر گربه بیت ۱، و به تصاویر سگ بیت ۱ را اختصاص میدهیم.

```
# First we should read all the images from the provided directory,

# 1. first unzip the .zip file attached with homeworks
!unzip "drive/MyDrive/data/HW3.zip"

# 2. read images from directory
images = []
dataset = os.listdir("./data_aug")

# 3. create labels array
labels=[]
for image in dataset:
    images.append(cv2.imread(os.path.join("./data_aug", image)))
    label = image.split('.')[0]
    if label == 'cat':
        labels.append(0)
    else:
        labels.append(1)
```

حال تصاویر را با تقسیم کردن بر ۲۵۵، نرمالیزه میکنیم تا عددی بین ۰ و ۱ به ما بدهد.

```
[ ] # Normalize your dataset in a way to have a image dataset with pixles in range (0 to 1)

images = np.divide(images, 255)
```

با استفاده از دستور cv2.resize، تصاویر خود را به سایز (۲۸ * ۲۸) در میآوریم.

```
[ ] # Resize your images to (28 * 28)

x_train = []
for image in images:
    x_train.append(cv2.resize(image, (28, 28)))
```

گام بعد، flatten کردن x_{train} و y_{train} مییاشد که چون از نوع list هستند، باید ابتدا به x_{train} تبدیل کرده و بعد flatten کنیم.

```
# Flatten your dataset images

x_train = np.array(x_train)
y_train = np.array(labels)
x_train = x_train.flatten().reshape(100, 2352)
y_train = y_train.flatten()
```

برای چک کردن سایز x_{train} و y_{train} ، از دستور x_{train} استفاده کرده و سایز آنها را پرینت میکنیم.

مدل خود را به صورت sequential تعریف می کنیم.

```
# create a simple model of Keras MLP with desired number of dense layers and units and activation function
# don't forget to shuffle the data
# this is a binary classification problem

model_temp_1 = Sequential()
model_temp_1.add(Dense(512, input_shape=(2352, ), activation='relu'))
model_temp_1.add(Dense(16, activation='relu'))
model_temp_1.add(Dense(1, activation='sigmoid'))
```

سپس با استفاده از دستور train_test_split دیتاست خود را به دادههای test و train و test میس با استفاده از دستور test به کل تقسیم کردیم. ورودی ها این تابع به ترتیب، داده، label مربوط به آن و نسبت test به کل داده می باشد که در اینجا ۳۳.۰ را به عنوان داده test و مابقی را برای train در نظر گرفتیم.

```
# Split your dataset to test and train with your desired implementation
# use sklearn.model_selection.train_test_split

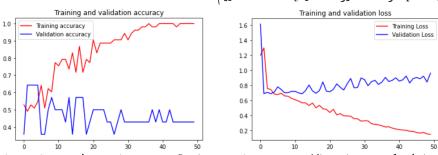
from sklearn.model_selection import train_test_split
x_train, x_test, y_train, y_test = train_test_split(x_train, y_train, test_size=0.33)
```

حال مدل خود را compile و fit میکنیم. چون در تمرین قبل (HW2) دیدیم که compile محل مدل خود را مدل خود را میکنیم. چون در تمرین قبل (Adam به عنوان Adam به عنوان مسبت به سایر بهینه سازها داشت، در اینجا از Adam به عنوان میکنیم و به دلیل دو کلاسه بودن، از optimizer میردیم.

```
# Compile with your desired optimizer and loss function with 'accuracy' as metric
# # Don't forget to monitor the overfitting, you should take care of val_accuracy and val_loss

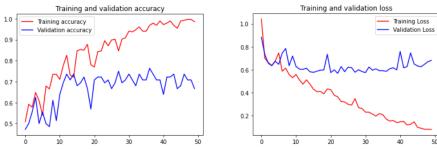
model_temp_1.compile(
    loss='binary_crossentropy',
    optimizer='adam',
    metrics=['accuracy']
)
history = model_temp_1.fit(
    x_train,
    y_train,
    epochs=50,
    validation_split=0.2,
    shuffle=True,
    verbose=2
)
```

با plot كردن مقادير loss و accuracy داريم:



همانطور که در تصاویر بالا نیز مشخص است، مدل overfit شده است. طبق نمودار، مقدار accuracy برای دادههای train به تدریج افزایش می یابد و loss آن کم می شود؛ اما مشکل آنجایی وجود دارد که روی دادههای validation، عملکرد خوبی ندارد و دقت آن دچار تنزل می شود و loss آن نیز افزایش می یابد. از دلایل این اتفاق، می توان به کم بودن تعداد train ریاد بودن ابعاد شبکه که موجب حفظ جزئیات دادههای train شده است و train بیش از حد اشاره کرد. در انتها، مدل خود را evaluate می کنیم.

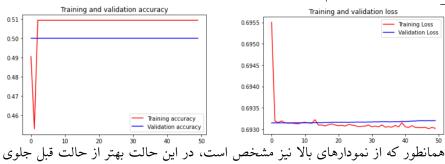
حال، از توابع تعریف شده استفاده کرده و دیتاست خود را افزایش میدهیم که ۸ برابر می شود. سپس مراحل قبل را تکرار کرده و accuracy و نمودارهای loss را plot میکنیم.



همانطور که در از نمودارها نیز مشخص است، مقدار دقت برای دادههای validation افزایش یافت و loss آن نیز نسبت به حالت قبل کمتر میباشد. این موضوع نشان می دهد با انجام این کار (داده افزایی) تا حدی جلوی overfitting را گرفتیم و برای جلوگیری بیشتر از این اتفاق، باید عوامل دیگر نظیر Dropout ،Regularizaton و غیره را نیز لحاظ کرد. در انتها مدل جدید خود را evaluate می کنیم.

از مقایسه نتیجه این بخش برای این مدل با نتیجه حاصل برای مدل قبل نیز، می بینیم که مقدار دقت ۰.۲۵ افزایش و ۱۰.۲۵ کاهش یافته است.

• ب) حال با استفاده از توابع آماده keras، مراحل قبل را انجام میدهیم. با plot کردن accuracy و loss و loss



همانطور که از نمودارهای بالا نیز مشخص است، در این حالت بهتر از حالت قبل جلوی overfitting گرفته شد؛ اما نکتهای که وجود دارد، این است که مقادیر دقت و loss تقریبا کاهش یافته است. حال مدل کنونی خود را evaluate میکنیم.

```
test_evaluate_3 = model_temp_3.evaluate(x_test_3, y_test_3)
print("Test evaluation is: ", test_evaluate_3)

2/2 [========] - 0s 9ms/step - loss: 0.6935 - accuracy: 0.4848
Test evaluation is: [0.6935147047042847, 0.4848484992980957]
```

همانطور که مشاهده می شود، مقدار loss و loss نسبت به حالت قبل، کاهش یافته است؛ اما نسبت به حالت اولیه، loss ۰.۳ کاهش و دقت حدود ۰.۱ افزایش داشته است. بنابراین نتیجه می گیریم مزیت استفاده از این روش نسبت به روش قبلی، کاهش بیشتر overfitting و افزایش عایب آن نسبت به روش قبل، می توان به کمتر شدن accuracy و افزایش loss اشاره کرد.

(قابل ذكر است كه مقدار accuracy و loss را با مدل قبل (mode_temp_2) مقايسه كرديم؛ مگرنه نسبت به مدل اوليه شاهد افزايش accuracy و كاهش loss بوديم.)

سوال ۴:

در MLP_Overfit.ipynb یک مدل MLP یک مدل MLP و یک مجموعهداده به شما داده شده است. این مدل بر روی مجموعة دادة داده شده، overfit شده است. با استفاده از ابزارهای موجود در کتابخانة keras سعی کنید از overfit شدن آن جلوگیری کنید. در نهایت نتایج به دست آمدة خود را گزارش کرده و تحلیل کنید. (۲۵ نمره) (حتماً با دلیل ذکر کنید که چرا مدل overfit بود و چرا با تغییرات انجام داده شده مدل در راستای حل آن گام برداشته است)

(توجه: استفاده از regularization و dropout مورد انتظار اما به راهکارهای اضافهتر که بتوانند نتایج بهتری نیز ثبت کنند نمرة امتیازی تعلق میگیرد.)

پاسخ ۴:

در ابتدا مدل خود را به صورت sequential طبق توضیحات داده شده، با ۳ لایه مخفی که هر unit ۱ دارای ۵۰ unit ۱ هستند و یک لایه خروجی حاوی ۱ unit و sigmoid activation function میسازیم.

```
# Create a Sequential MLP model with these Dense layers:
# 3 hidden layers with 50 units each and 'relu' activation
# 1 unit output with 'sigmoid' activation

model = Sequential()

# Hidden Layer
model.add(Dense(units=50, activation="relu"))
model.add(Dense(units=50, activation="relu"))
model.add(Dense(units=50, activation="relu"))

# Output Layer
model.add(Dense(units=1, activation="sigmoid"))
```

سپس با استفاده از دستور train_test_split دیتاست خود را به دادههای test و train تقسیم کردیم. ورودی ها این تابع به ترتیب، داده، label مربوط به آن و نسبت test می باشد که در اینجا ۳۳.۰ را به عنوان داده test و مابقی را برای train در نظر گرفتیم.

```
# Split your dataset to test and train with your desired implementation
# use sklearn.model_selection.train_test_split

X_train, X_test, y_train, y_test = train_test_split(sgx, sgy, test_size=0.33)
```

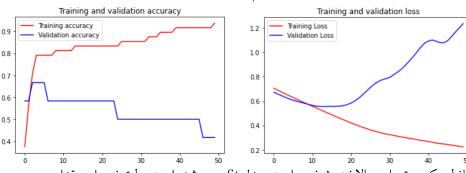
در ادامه مدل خود را با استفاده از BinaryCrossentropy loss function و BinaryCrossentropy را accuracy با 1.0 metrics میکنیم. (طبق توضیحات داده شده، metrics میگذاریم)

```
[95] # Compile with your desired optimizer and loss function with 'accuracy' as metric
    # Don't forget to monitor the overfitting, you should take care of val_accuracy and val_loss
    model.compile(
        loss = 'binary_crossentropy',
        optimizer = 'adam',
        metrics = ['accuracy']
    )
```

حال مدل خود را fit كرده و validation_split را ۰.۲ (طبق گفته سوال) قرار مي دهيم.

```
# Start training and fit your model with desired parameters and validation_split=0.2
history = model.fit(
    x = sgx,
    y = sgy,
    epochs = 50,
    validation_split = 0.2,
    verbose=0,
)
```

با plot كردن مقادير loss و accuracy داريم:



همانطور که در تصاویر بالا نیز مشخص است، مدل overfit شده است. طبق نمودار، مقدار مقدار معدار برای داده های train به تدریج افزایش می یابد و loss آن کم می شود؛ اما مشکل آنجایی وجود دارد که روی داده های validation، عملکرد خوبی ندارد و دقت آن دچار تنزل می شود و loss آن نیز افزایش می یابد. از دلایل این اتفاق، می توان به کم بودن تعداد dataset، زیاد بودن ابعاد شبکه که موجب حفظ جزئیات داده های train شده است و train بیش از حد اشاره کرد. در انتها، مدل خود را و evaluate می کنیم.

برای بهبود مدل و کاهش overfitting، می توانیم از روشهای اضافه کردن اروشهای داد اضافه کردن ابعاد شبکه (تعداد تعداد نمونههای موجود در دیتاست، کم کردن نورونهای هر لایه و کم کردن ابعاد شبکه (تعداد لایهها) اشاره کرد. برای کم کردن overfitting تمامی این روشها را اعمال می کنیم. در ابتدا hyperparameter او ایرای L_2 ، L_1 و Dropout تعریف می کنیم.

```
[4] 11 = 0.0005
12 = 0.005
p = 0.5
```

سپس به منظور جلوگیری از overfitting، تعداد نمونهها را افزایش میدهیم؛ زیرا یکی از دلایل بروز overfitting، کم بودن تعداد نمونههای موجود در دیتاست میباشد.

```
sgx, sgy = make_sample(200)

plt.scatter(sgx[:,0], sgx[:,1], alpha=0.5, c=sgy)
plt.xlabel('x1')
plt.ylabel('x2')
```

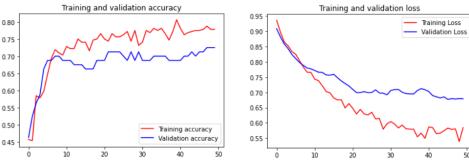
در ادامه با کم کردن ابعاد شبکه (تغییر تعداد لایهها از ۴ به ۳) و کم کردن نورونهای موجود در هر لایه، به کاهش overfitting کمک میکنیم.

```
model = Sequential([
    Dense(32, activation='relu', kernel_regularizer=L1L2(l1, l2)),
    Dropout(p),
    Dense(16, activation='relu', kernel_regularizer=L1L2(l1, l2)),
    Dropout(p),
    Dense(1, activation='sigmoid', kernel_regularizer=L1L2(l1, l2)),
])
```

این بار، بخش کوچکتری از دیتاست را برای test جدا میکنیم.

```
[71] x_train, x_test, y_train, y_test = train_test_split(sgx, sgy, test_size=0.1)
```

سپس مدل خود را compile و fit كرده و نتايج accuracy و loss آن را مشاهده ميكنيم.



همانطور که در تصاویر بالا نیز مشخص است، مقادیر loss و accuracy برای دادههای validation تا حد زیادی بهبود پیدا کرد و دقت و loss برای دادههای train و validation نسبتا همگرا شد که نشان می دهد مدل ما از حالت overfitting تقریبا خارج شده است.

با اضافه کردن تعداد نمونهها، باعث شدیم تا مدلمان روی یک سری داده محدود fit نشود و با استفاده

از نمونههای بیشتری تصمیمگیری کند. با کم کردن تعداد لایهها و نورونها، موجب کاهش ظرفیت یادگیری مدل شدیم تا فقط ویژگیهای برجسته را حفظ کند و به جزئیات کاری نداشته باشد. با استفاده از جریمه کردن پارامترها (L_2 و L_1) باعث محدود کردن پارامترهای مدل، به منظور محدود کردن ظرفیت یادگیری شدیم. Dropout نیز به نوعی با استفاده از داده افزایی از overfitting جلوگیری میکند. سپس با کاهش تعداد نمونههای انتخابی برای test و اختصاص بخش بزرگ تر برای باز هم موجب داده افزایی شدیم.

با evaluate کردن مدل جدیدمان، مطابق انتظار، مقدار accuracy برای داده test افزایش و مقدار loss آن کاهش می یابد که نشان می دهد خوب عمل کردیم.