بسمه تعالی



دانشکده مهندسی کامپیوتر

**یادگیری عمیق**

نام استاد: دکتر محمدی

تمرین هشتم

آرمان حیدری

شماره دانشجویی: **97521252**

آذر **1400**

# پاسخ سوال اول

**الف)** استفاده اصلی لایه dropout برای جلوگیری از overfit شدن مدل است. کار این لایه این است که به صورت رندوم در هنگام آموزش، وزن تعدادی از نورون ها را صفر میکند. پارامتر نگهداری نورون ها عددی بین 0 و 1 است که درواقع احتمال صفر شدن وزن نورون در هر epoch زمان آموزش را نشان میدهد. مثلا اگر بعد از یک لایه که 100 نورون دارد یک لایه dropout با p=0.4 قرار دهیم، انگار در هر آموزش به صورت رندوم 40 تا از نورون ها تاثیری روی خروجی نمیگذارند.

این لایه ازین که تمام نورون ها به صورت موازی به یک هدف آپدیت شوند جلوگیری میکند و در نتیجه شبکه کمتر به مقادیر دقیق هر نورون وابسته شده و overfit نمیشود. همچنین در صورت کار نکردن یکی از نورون ها به هر دلیلی، مدل قبلا چنین شرایطی را داشته و موقع تست دچار خطای زیادی نمیشود.

**ب)** اگر مقدار پارامتر نگهداری شبکه در dropout با همان P، زیاد شود به معنی صفر شدن بیشتر نورون های آن لایه است. و در نتیجه capacity شبکه که به معنی تعداد نورون های شبکه (تعداد لایه ها و نورون های هر لایه) است کاهش میابد. و با استدلال مشابه با کاهش p، Capacity زیاد می شود و درواقع رابطه معکوس دارند.

معمولا احتمال dropout را عددی بین 0.2 تا 0.5 میگذارند. چون مقادیر کمتر عملا تاثیری ندارند و مقادیر بیشتر هم استفاده از نورون های زیاد هر لایه را بیهوده میکنند. چون اگر dropout زیاد باشد، انگار نورون های شبکه کم هستند و شبکه به خوبی نمی تواند روی داده آموزشی fit شود.

**منابع:** [medium.com](https://medium.com/jun-devpblog/dl-1-learning-algorithms-and-basic-terms-of-dl-65d46ceb1b0a#:~:text=In%20the%20neural%20networks%2C%20the,consists%20of%20one%20linear%20layer.)، [keras.io](https://keras.io/api/layers/regularization_layers/dropout/#:~:text=The%20Dropout%20layer%20randomly%20sets,over%20all%20inputs%20is%20unchanged.)، [oreilly.com](https://www.oreilly.com/library/view/machine-learning-for/9781786469878/252b7560-e262-49c4-9c8f-5b78d2eec420.xhtml#:~:text=The%20main%20advantage%20of%20this,goal%2C%20thus%20decorrelating%20the%20weights.)

# پاسخ سوال دوم

* Fullty connected layer: نوع لایه هایی که تا اینجای درس با آن ها سر و کار داشتیم است. که در tensorflow به عنوان Dense شناخته می شود. این لایه تعدادی نورون دارد که هر کدام وزن مخصوص به خود را دارند و یک bias هم برای آن ها وجود دارد. در این نوع لایه، تمام نورون(پیکسل) های ورودی به تمام نورون های لایه تماما متصل وصل می شوند. برای مسائل classification و به خصوص لایه های انتهایی یک شبکه عمیق بسیار کاربردی هستند.
* Convolutional layer: نقش یک لایه کانولوشن شناسایی ویژگی های محلی در موقعیت های مختلف از نقشه های ویژگی ورودی با filterها و kernel ها قابل یادگیری است. با این لایه درواقع روی مرتبط بودن اجزای مختلف یک ورودی حساب میکنیم و یک فیلتر خاص را روی نقاط مختلف آن پیاده میکنیم. مثلا برای شناسایی ویژگی خاصی در یک تصویر یا یک صوت میتوان از یک لایه کانوولوشنی استفاده کرد. ویژگی مهم آن ها پارامترهای کم قابل یادگیری هم هست. پارامترهای stride و padding و kernel size این لایه باید مشخص باشد.
* Locally connected layer: این نوع لایه کاملاً مشابه لایه Convolutional است اما تنها با یک تفاوت (مهم). در لایه Convolutional فیلتر در بین تمام نورون های خروجی (پیکسل) مشترک بود. به عبارت دیگر، ما از یک فیلتر واحد برای محاسبه تمام نورون ها (پیکسل) یک کانال خروجی استفاده کردیم. با این حال، در Locally-Connected Layer هر نورون (پیکسل) فیلتر مخصوص به خود را دارد. این بدان معناست که تعداد پارامترها در تعداد نورون های خروجی ضرب می شود. این می تواند به شدت تعداد پارامترها را افزایش دهد و اگر داده کافی نداشته باشید، ممکن است با overfitting مواجه شوید. با این حال، این نوع لایه به شبکه شما اجازه می دهد تا انواع مختلفی از ویژگی ها را برای مناطق مختلف ورودی یاد بگیرد. محققان از این ویژگی مفید لایه های محلی متصل به ویژه در تأیید چهره مانند DeepFace و DeepID3 استفاده کردند. با این حال، برخی دیگر از محققان از یک فیلتر مجزا برای هر ناحیه از ورودی به جای هر نورون (پیکسل) استفاده می‌کنند تا از لایه‌های محلی متصل با تعداد پارامترهای کمتر بهره ببرند.

**منابع:** [medium](https://medium.com/machine-learning-for-li/different-convolutional-layers-43dc146f4d0e)

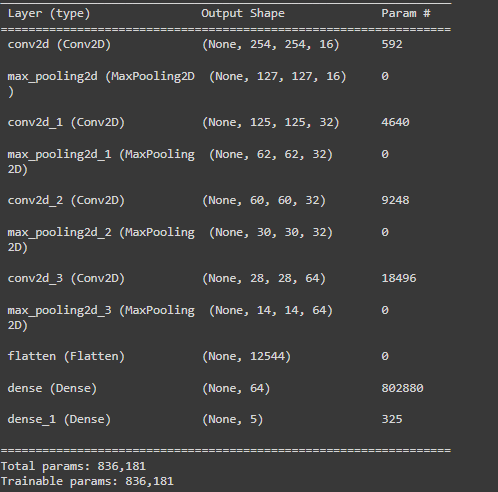
# پاسخ سوال سوم

کدهای مربوط به این سوال در HW8.ipynb ضمیمه شده است. [(لینک گوگل کولب)](https://colab.research.google.com/drive/1EjouNEq4uu_Fht0a7Dxx9O03lsyNN25n?usp=sharing)

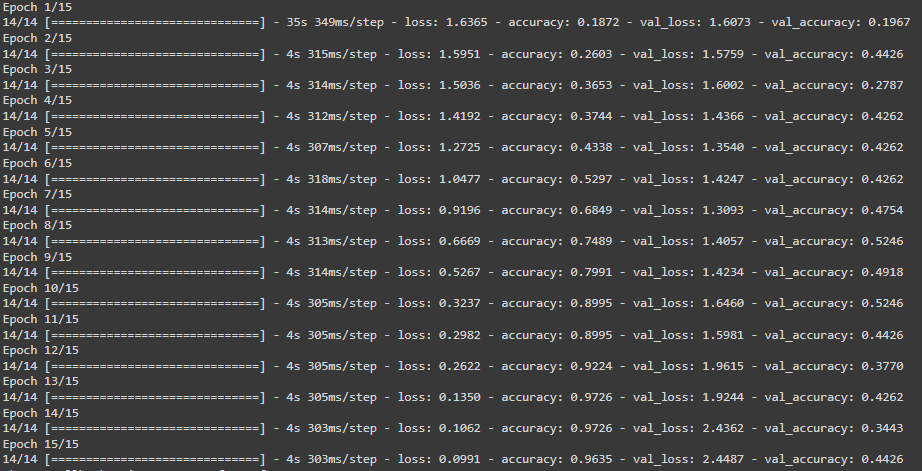
**الف)** در این بخش فقط باید داخل تابع flow\_from\_directory را برای validation\_datagen و train\_datagen پر میکردیم تا داده های آموزشی و ارزیابی را بدون مشکل تشکیل دهیم. این کار را فعلا بدون data augmentation انجام دادیم.

در این سوال داده ارزیابی و تست را یکی در نظر گرفته ایم.

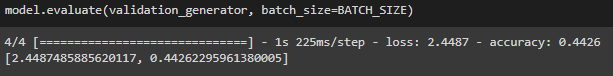
**ب)** مدل را با 4 لایه کانوولوشنی که پس از هر کدام یک لایه maxpooling با ابعاد و stride، (2,2) پس از هر کدام میسازیم تا پارامترها و زمان اجرا خیلی زیاد نشود. به نوعی از overfit هم جلوگیری کند. بعد هم مطابق صورت سوال از دو لایه Dense استفاده میکنیم. نکته مهم این است که دومی به تعداد کلاس ها (5) نورون داشته باشد و تابع فعالسازی آن softmax باشد. مدل را با بهینه ساز آدام که بهترین است و تابع ضرر categorical crossentropy چون مسئله چندین کلاسه است، اجرا میکنیم.



با این هایپرپارامتر های معقول میبینیم که مدل overfit میکند. از نتایج که دقت آموزش به عدد بالایی رسیده و دقت ارزیابی پایین است مشخص است:



و در نهایت نتیجه سلولی که برای ارزیابی اجرا میکنیم:



که دقت پایینی است و در مقایسه با 96 درصد داده آموزشی، overfit مدل واضح است.

**پ)** تفاوت این بخش در دادن ورودی به ImageDataGenerator است. میخواهیم داده بیشتری از هر کلاس داشته باشیم و این کار را با چرخاندن عکس، جابجایی عرضی آن، جابجایی افقی آن، زوم کردن روی بخشی از عکس، بریدن افقی بخشی از عکس انجام میدهیم. به این طریق مدل نسبت به عکس های کم bias نمیشود و نویز ها اثر کمتری روی تصمیم گیری آن میگذارند. نوع data augmentation ما به این صورت است:

train\_datagen = ImageDataGenerator(

    rescale=1./255,

    rotation\_range=40,

    width\_shift\_range=0.2,

    height\_shift\_range=0.2,

    shear\_range=0.2,

    zoom\_range=0.2,

    horizontal\_flip=True,

    fill\_mode='nearest')

test\_datagen = ImageDataGenerator(

    rescale=1./255,

    rotation\_range=40,

    width\_shift\_range=0.2,

    height\_shift\_range=0.2,

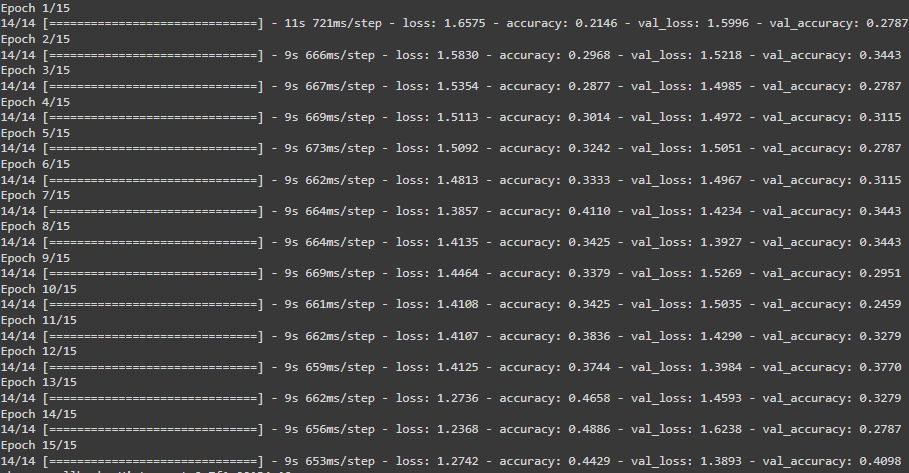
    shear\_range=0.2,

    zoom\_range=0.2,

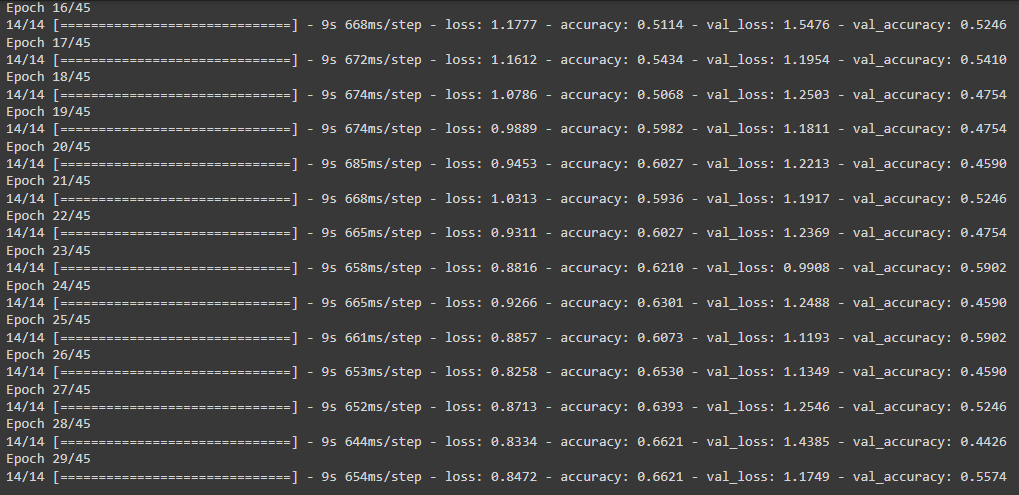
    horizontal\_flip=True,

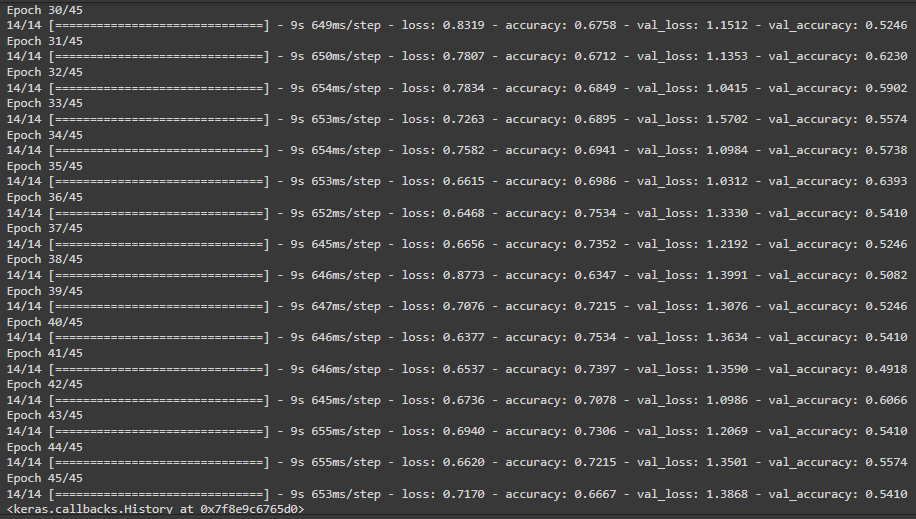
    fill\_mode='nearest')

با 15 بار اجرا (مثل قسمت قبلی) میبینیم که مدل همچنان fit نشده است و نیاز به اجرای بیشتری دارد. که با توجه به افزایش قابل توجه داده های آموزشی امری طبیعی است.



پس آموزش را ادامه میدهیم:





مشخص است که شبکه از نظر overfit شدن نسبت به قسمت الف شرایط بسیار بهتری دارد. دقت روی داده آموزشی در اینجا بالا میرود چون شبکه موارد بیشتری را میبیند. دقت validation هم در جاهایی از آموزش کمی بهتر شده اما بازهم عدد قابل توجهی نیست.

حال برای مقایسه، نوع ساختن دیتاهای جدیدمان را تغییر میدهیم. و به این صورت تعریف میکنیم:

train\_datagen = ImageDataGenerator(

    rescale=1./255,

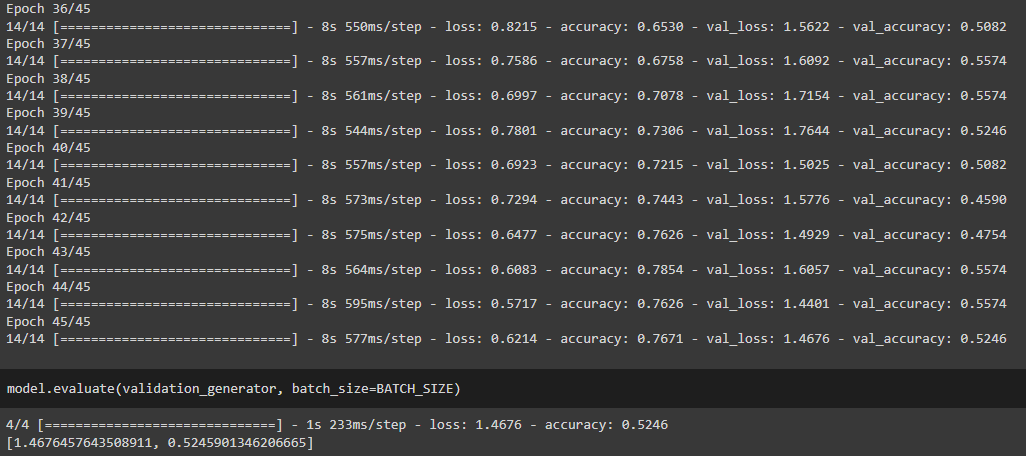
    shear\_range=0.2,

    zoom\_range=0.3,

    horizontal\_flip=True)

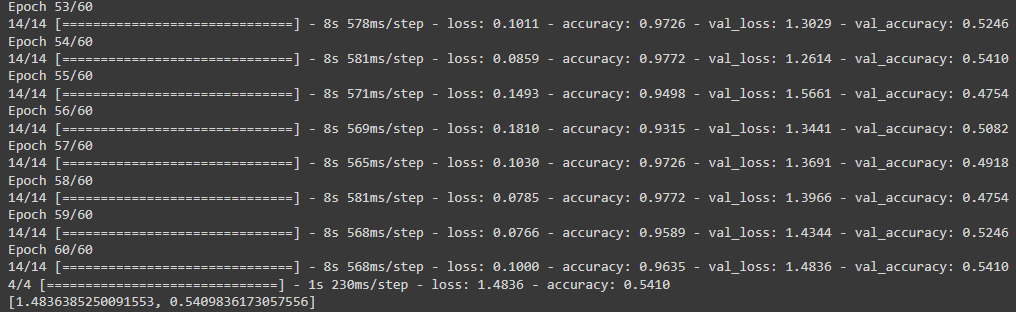
test\_datagen = ImageDataGenerator(rescale=1./255)

در واقع داده های تست را دیگر تغییری نمیدهیم و سعی میکنیم داده های آموزشی هم با تغییرات کمتری generate کنیم. چون شاید در مثال قبلی در این امر زیاده روی کرده بودیم. نتایج به این صورت به دست آمد:

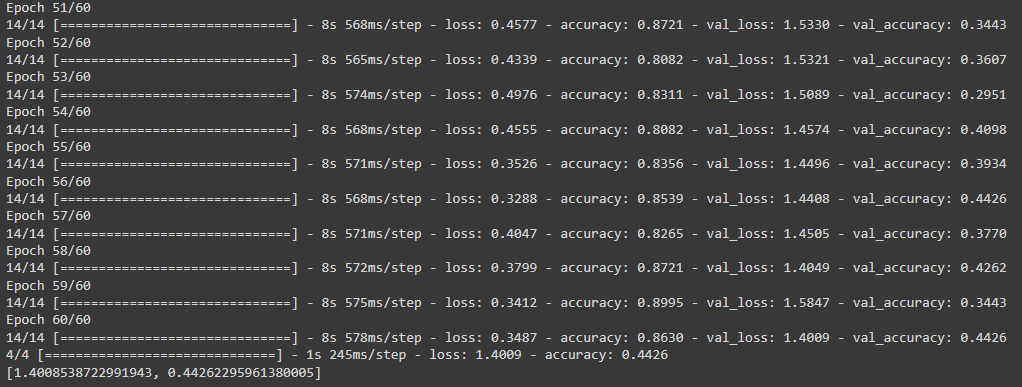


اوضاع از حالات قبلی بهتر شد اما همچنان با توجه به اختلاف دقت بالای داده آموزشی و ارزیابی، overfit شدن را داریم. در قسمت بعدی با اضافه کردن dropout سعی میکنیم این مشکل را تا حدی حل کنیم.

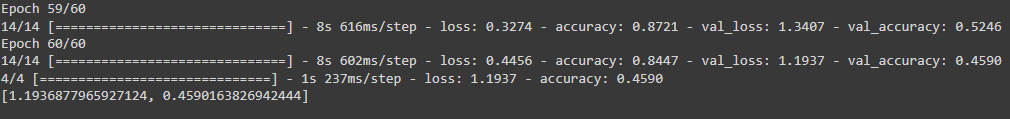
**ت)** پس از تمام لایه های کانوولوشن، یک لایه dropout اضافه میکنیم. با احتمالات مختلفی برای dropout این سوال را حل میکنیم. البته data augmentation و سایر هاپرپارامترها را ثابت در نظر میگیریم و فقط احتمال dropout را به عنوان ورودی به تایع build\_model میدهیم. ابتدا احتمال را برابر 0.25 میگذاریم تا هر بار موقع آموزش فقط یک چهارم نورون ها صفر شوند. نتایج به این صورت به دست می آید:



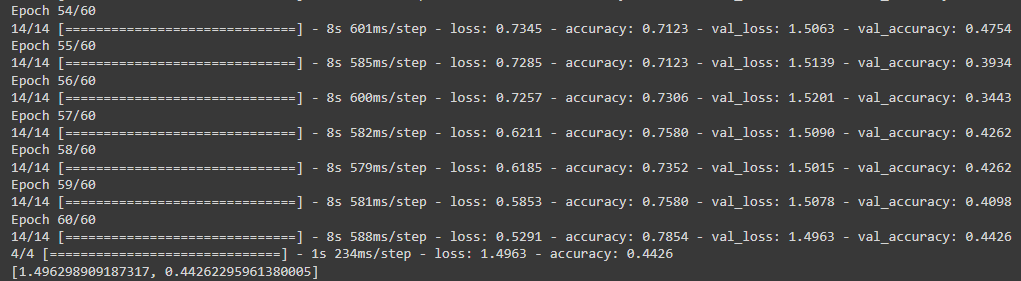
نتایج از دفعات قبل بهتر شده است اما همچنان overfit را داریم. پس احتمال dropout را به 0.5 افزایش میدهیم:



همچنین با نرخی بین این دو عدد یعنی 0.4 هم امتحان کردم و به چنین نتیجه ای رسیدم:



که متاسفانه در هیچکدام ازین حالات مشکل overfit شدن حل نشد. پس با عددی بیش از مقدار معمول یعنی 0.7 امتحان کردم که به نتایج زیر رسید:



نتایج روی validation بهبود خاصی نداشتند و صرفا دقت آموزشی کم شده است.

برای حل مشکل overfit در این سوال، با ساختن دیتا ها و اضافه کرد dropout پیشرفت کردیم اما همچنان به ظور کامل رفع نشد. احتمالا باید از روش های دیگری مانند kernel regularizer استفاده میکردیم.

**د)** برای این قسمت بهترین مدل قسمت قبل را در نظر میگیریم. (آخرین مدلی که تعریف شد و dropout=0.25)

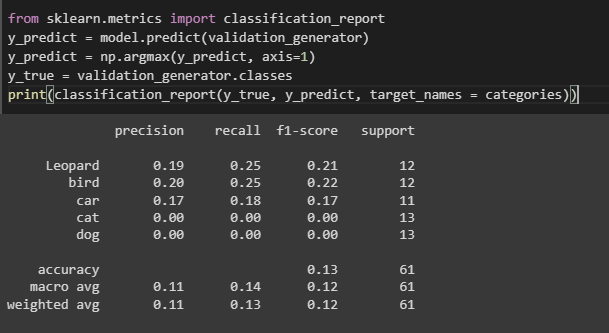
* Precision: معیار خوبی برای تعیین زمانی است که هزینه های مثبت کاذب زیاد است. به عنوان مثال، تشخیص هرزنامه ایمیل. در تشخیص اسپم ایمیل، مثبت کاذب به این معنی است که ایمیلی که غیر اسپم است (منفی واقعی) به عنوان اسپم (اسپم پیش بینی شده) شناسایی شده است. اگر دقت در مدل تشخیص اسپم بالا نباشد، کاربر ایمیل ممکن است ایمیل های مهم را از دست بدهد.
* Recall: در واقع محاسبه می کند که مدل ما چه تعداد از مثبت های واقعی را از طریق برچسب گذاری آن به عنوان مثبت (مثبت واقعی) گرفته است. با استفاده از همین درک، می دانیم که Recall معیاری است که برای انتخاب بهترین مدل خود در زمانی که هزینه زیادی با False Negative وجود دارد، استفاده می کنیم.

به عنوان مثال، در تشخیص تقلب بانکی. اگر تراکنش متقلبانه (Actual Positive) به عنوان غیر متقلبانه (Predicted Negative) پیش بینی شود، عواقب آن می تواند برای بانک بسیار بد باشد.

به طور مشابه، در تشخیص بیماری حاد. اگر یک بیمار (Actual Positive) آزمایش را انجام دهد و پیش بینی شود که بیمار نباشد (Predicted Negative). اگر بیماری مسری باشد، هزینه مربوط به منفی کاذب بسیار بالا خواهد بود.

* F1-score: زمانی مورد نیاز است که می‌خواهید تعادلی بین دقت و فراخوانی ایجاد کنید. قبلاً دیده‌ایم که دقت می‌تواند تا حد زیادی توسط تعداد زیادی از منفی‌های واقعی ایجاد شود که در بیشتر شرایط تجاری، ما روی آن تمرکز زیادی نداریم، در حالی که منفی کاذب و مثبت کاذب معمولاً هزینه‌های تجاری دارند (محسوس و ناملموس) بنابراین امتیاز F1 ممکن است یک امتیاز باشد. اگر نیاز به تعادل بین دقت و یادآوری داریم و توزیع کلاسی ناهمواری وجود دارد (تعداد زیادی از منفی های واقعی)، معیار بهتری برای استفاده است.

در این سوال با تابعی که پیشنهاد شده بود این مقادیر را حساب کردم و به این صورت به دست آمد:



**منابع:** [towardsdatascience](https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9)

**ه)** confusion matrix خلاصه ای از نتایج پیش بینی در مورد یک مسئله طبقه بندی است. تعداد پیش‌بینی‌های صحیح و نادرست با مقادیر شمارش خلاصه شده و بر اساس هر کلاس تجزیه می‌شوند. ماتریس Confusion یک ماتریس N x N است که برای ارزیابی عملکرد یک مدل طبقه‌بندی استفاده می‌شود، که در آن N تعداد کلاس‌های هدف است. ماتریس مقادیر هدف واقعی را با مقادیر پیش بینی شده توسط مدل یادگیری ماشین مقایسه می کند.

در این مثال با استفاده از تابعی که صورت سوال پیشنهاد داد این ماتریس را به این صورت به دست آوردم:

