Captcha Recognition

Group Members :-

- ❑ Yatharth (2017UCO1578)
- ❑ Siddharth (2017UCO1571)

Contents

- 1. Introduction to Neural networks
- 2. Digit Recognition using ANN
- 3. What is a Captcha ?
- 4. How Captcha Recognition Works ?
- 5. Conclusion

Artificial Neural Network

INTRODUCTION

- Neural“ is an adjective for neuron, and “network” denotes a graph like structure.

- Artificial Neural Networks are also referred to as “neural nets” , “artificial neural systems”, “parallel distributed processing systems”, “connectionist systems”.

- For a computing systems to be called by these pretty names, it is necessary for the system to have a labeled directed graph structure where nodes performs some simple computations.

- “Directed Graph” consists of set of “nodes”(vertices) and a set of “connections”(edges/links/arcs) connecting pair of nodes.

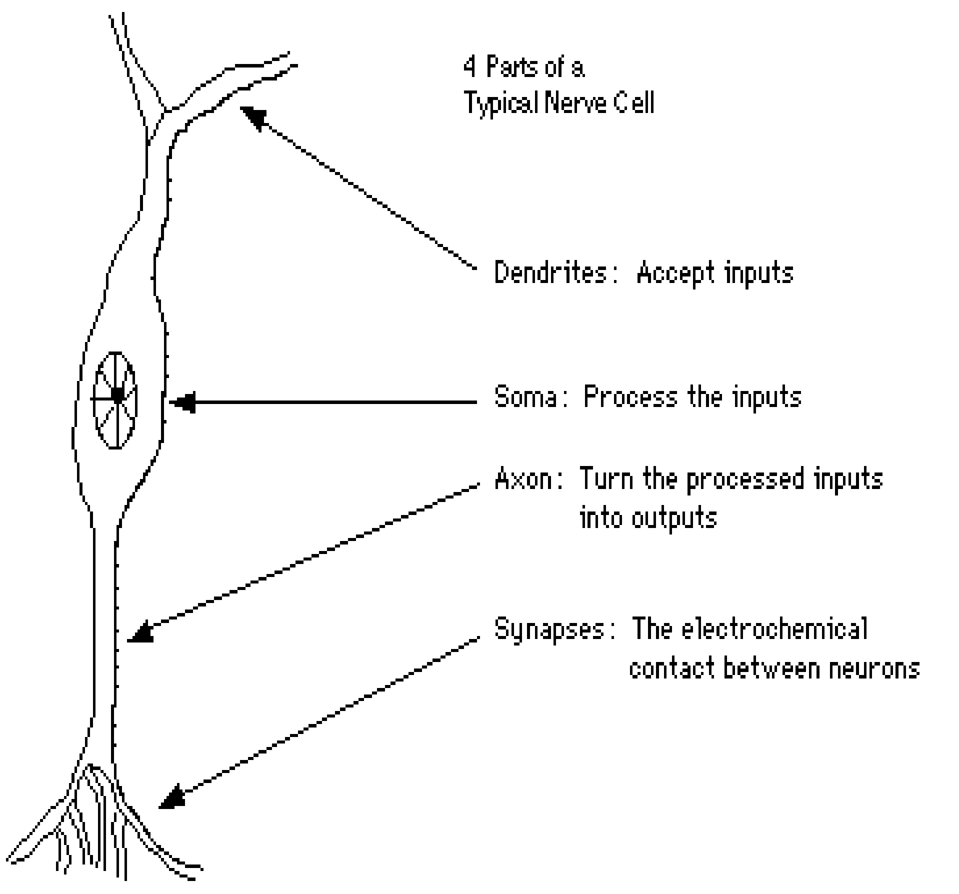
- A graph is said to be “labeled graph” if each connection is associated with a label to identify some property of the connection

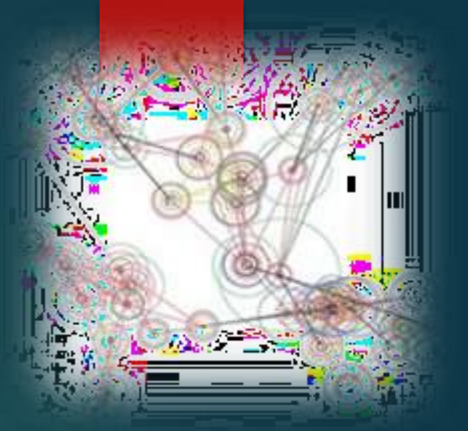
- The field of neural network was pioneered by BERNARD WIDROW of Stanford University in1950’s.

BIOLOGICAL NEURON MODEL

- **Four parts of a typical nerve cell : -**

- DENDRITES: Accepts the inputs
- SOMA : Process the inputs
- AXON : Turns the processed inputs into outputs.
- SYNAPSES : The electrochemical contact between the neurons.


4 Parts of a
Typical Nerve Cell
Dendrites : Accept inputs
Soma : Process the inputs
Axon : Turn the processed inputs
into outputs
Synapses : The electrochemical
contact between neurons

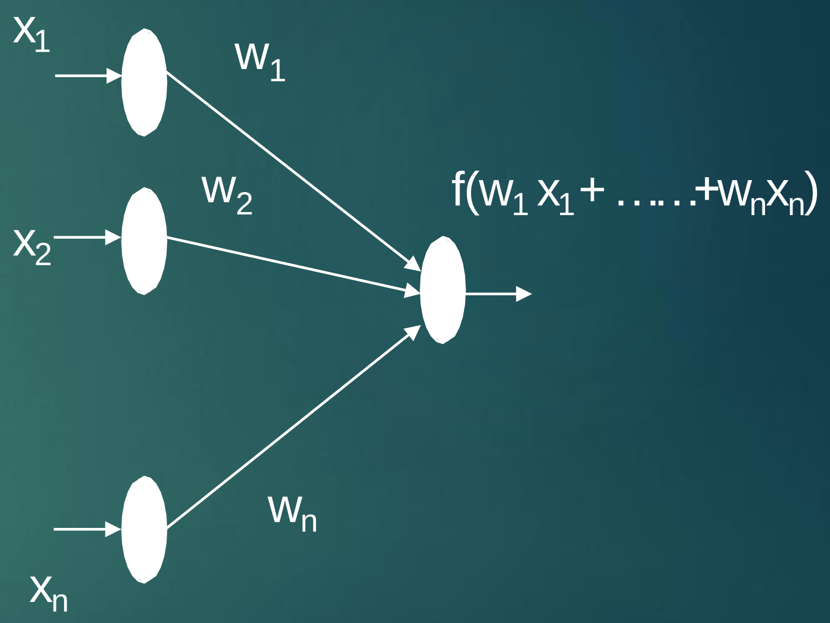


ARTIFICIAL NEURON MODEL

- Inputs to the network are represented by the mathematical symbol, x_n
- Each of these inputs are multiplied by a connection weight , w_n

$$\text{sum} = w_1 x_1 + \ldots\ldots + w_n x_n$$

- These products are simply summed, fed through the transfer function, f( ) to generate a result and then output.



Biological Terminology	Artificial Neural Network Terminology
Neuron	Node/Unit/Cell/Neurode
Synapse	Connection/Edge/Link
Synaptic Efficiency	Connection Strength/Weight
Firing frequency	Node output

- **Artificial Neural Network (ANNs)** are programs designed to solve any problem by trying to mimic the structure and the function of our nervous system.
- Neural networks are based on simulated neurons, Which are joined together in a variety of ways to form networks.
- Neural network resembles the human brain in the following two ways:-
    - A neural network acquires knowledge through learning.
    - A neural network's knowledge is stored within the interconnection strengths known as synaptic weight.

ARTIFICIAL NEURAL NETWORK MODEL

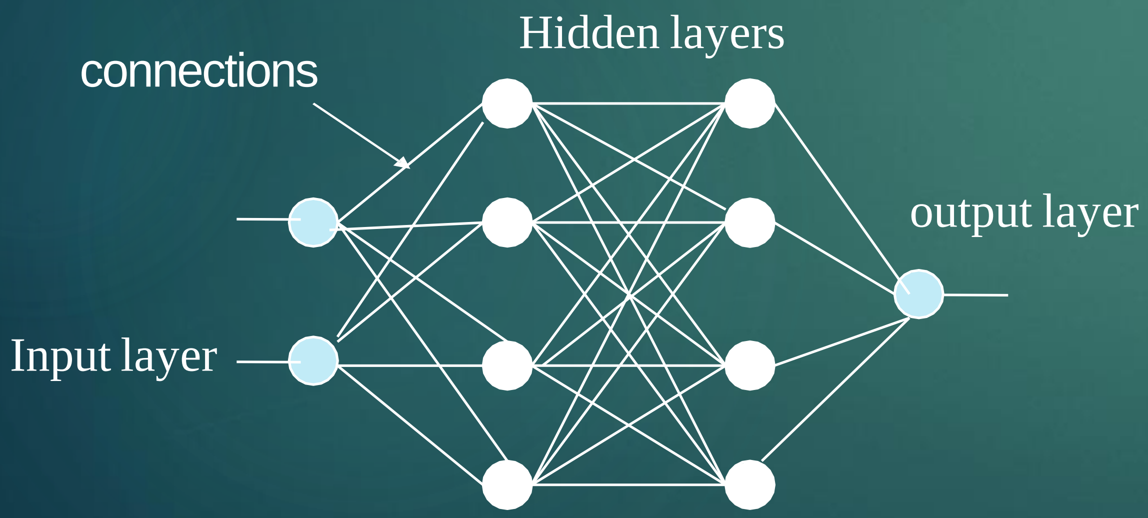
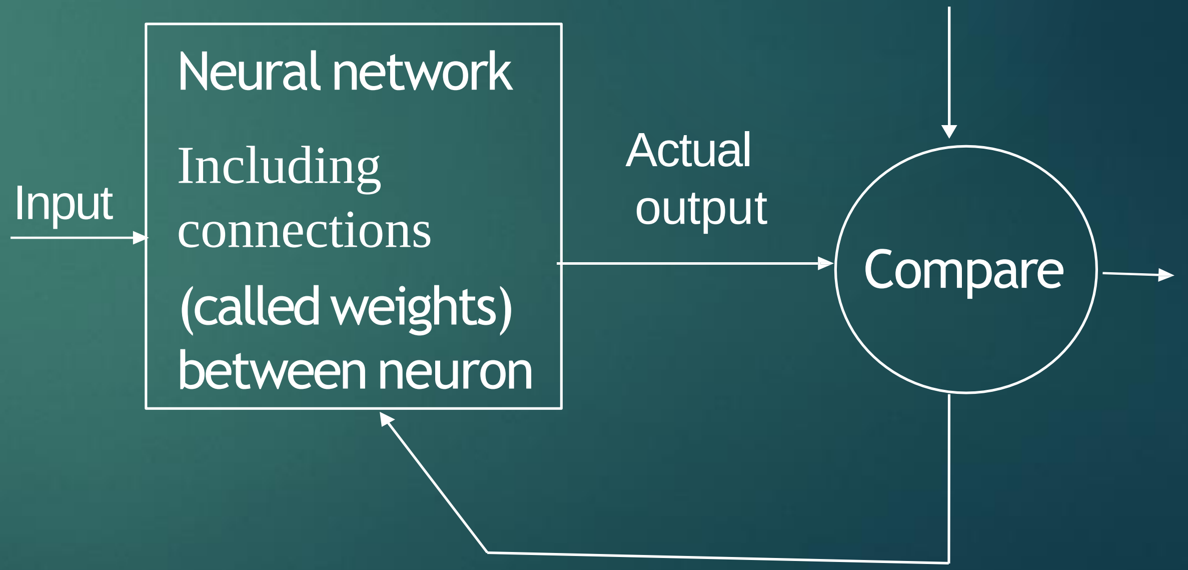


Fig 1: artificial neural network model



Input

Neural network

Including connections

(called weights) between neuron

Actual output

Compare

Figure showing adjust of neural network

NEURAL NETWORK ARCHITECTURES

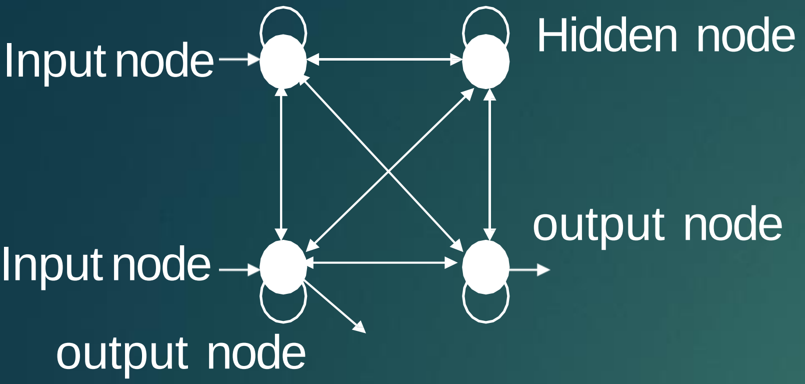


Fig: fully connectednetwork

The neural network in which every node is connected to every other nodes, and these connections may be either excitatory (positive weights), inhibitory (negative weights), or irrelevant (almost zero weights).

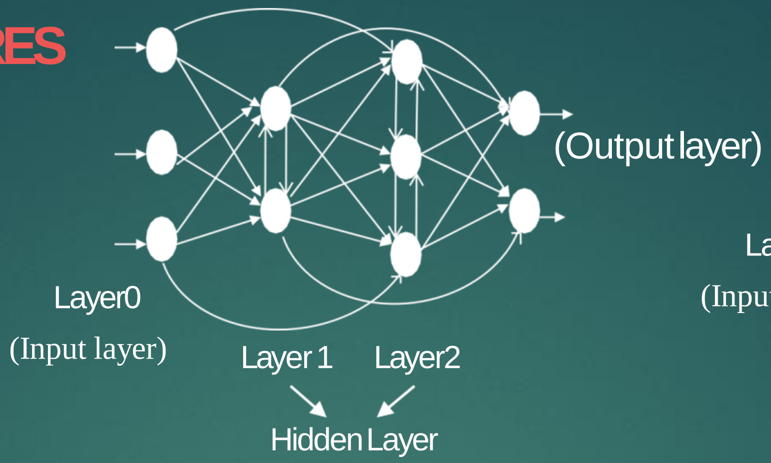


fig: layered network

These are networks in which nodes are partitioned into subsets called layers, with no connections from layer j to k if j > k.

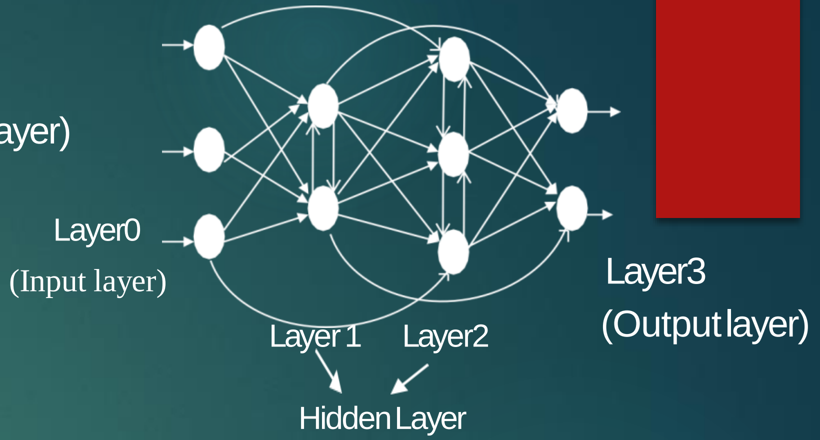


Fig :Acyclic network

This is the subclass of the layered networks in which there is no intra-layer connections. In other words, a in layer i and any node in layer j for i <j, but a connection is not allowed for i=j.

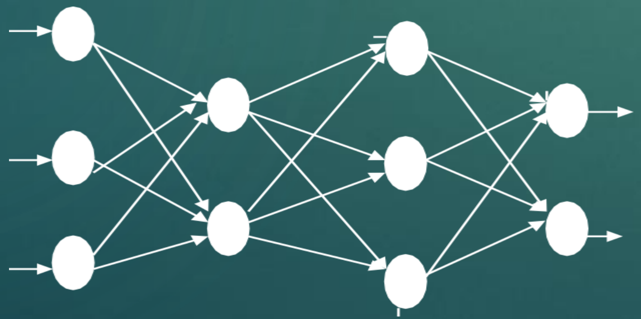


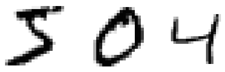
fig : Feedforward network

This is a subclass of acyclic networks in which a connection is allowed from a node in layer i only to nodes in layer i+1

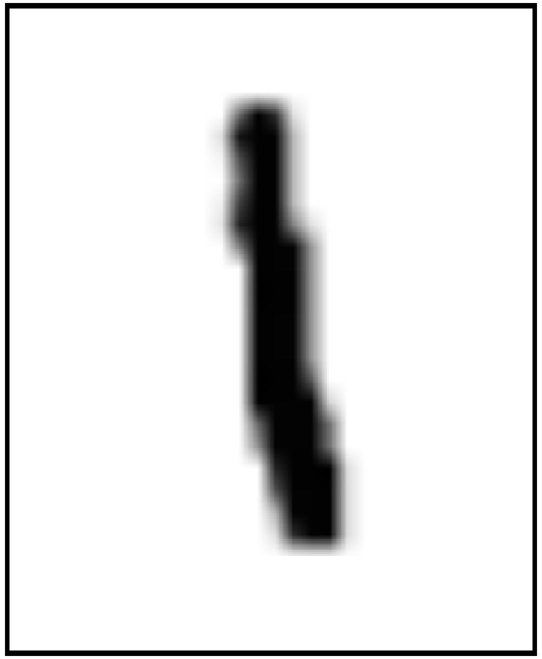
How Digit recognition Works ?

MNIST

MNIST is a simple computer vision dataset. It consists of 28x28 pixel images of handwritten digits, such as:



Every MNIST data point, every image, can be thought of as an array of numbers describing how dark each pixel is. For example, we might think as something like:



$$\cong \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & .6 & .8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & .7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & .7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & .5 & 1 & .4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & .4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & .4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & .7 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & .9 & 1 & .1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & .3 & 1 & .1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

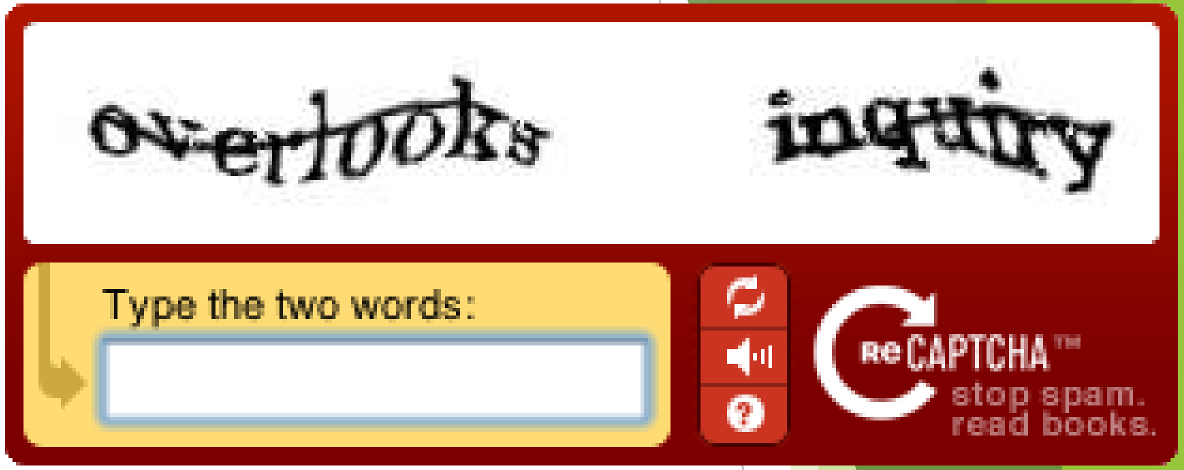
Since each image has 28 by 28 pixels, we get a 28x28 array. We can flatten each array into a 28∗28=78428∗28=784 dimensional vector. Each component of the vector is a value between zero and one describing the intensity of the pixel. Thus, we generally think of MNIST as being a collection of 784-dimensional vectors.

So this MNIST dataset will be divided into 2 parts , the first half will be used for training the ANN and the second half will be used for testing and finding the accuracy of the model.

What is a Captcha ?

CAPTCHA: Telling Humans and Computers Apart Automatically

A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text as the one shown, but current computer programs can't:



Applications of CAPTCHAs:

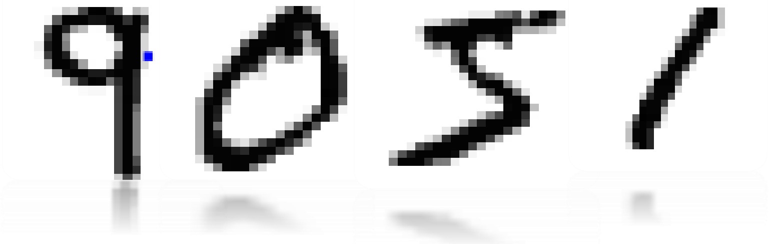
- **Protecting Website Registration.** Several companies (Yahoo!, Microsoft, etc.) offer free email services. Up until a few years ago, most of these services suffered from a specific type of attack: "bots" that would sign up for thousands of email accounts every minute. The solution to this problem was to use CAPTCHAs to ensure that only humans obtain free accounts. In general, free services should be protected with a CAPTCHA in order to prevent abuse by automated scripts.
- **Protecting Email Addresses From Scrapers.** Spammers crawl the Web in search of email addresses posted in clear text. CAPTCHAs provide an effective mechanism to hide your email address from Web scrapers. The idea is to require users to solve a CAPTCHA before showing your email address.
- **Preventing Dictionary Attacks.** CAPTCHAs can also be used to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins. This is better than the classic approach of locking an account after a sequence of unsuccessful logins, since doing so allows an attacker to lock accounts at will

How Captcha Recognition Works ?

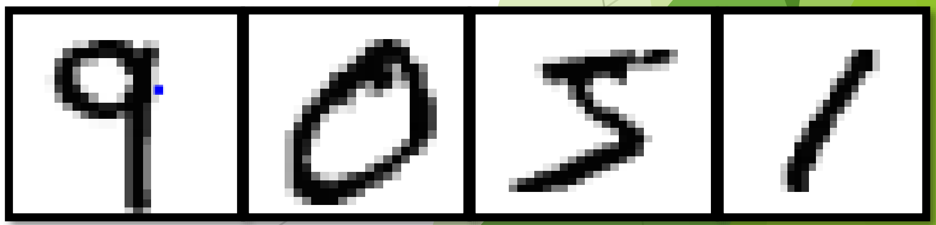
Captcha recognition works in the similar way as the digit recongnition. The only difference comes in the length. In captcha recognition the model will have to predict the entire sting correctly to identify the captcha.

Captcha’s that we will be using will consist of all possible combinations of 4 digit numbers . The captcha will not contain any other characters except numeric.

1. Our code will take the captcha (4 digit number image) and divide it into 4 parts so that individual digits can be obtained.
2. Then the learner (ANN model) will individually take the digits of the captcha and perform the prediction on them.
3. Finally the learner will output the individual digits of the captcha as the prediction is performed and at the end the output (complete captcha) will be obtained.



Original Captcha



After Division

Conclusion

- **Captchas** are vulnerable **to** attacks. A so called good **captcha** scheme **can** broken with an overall (segmentation and then **recognition**) **success** rate of more than 60%. Therefore, we find that **captchas** provide only a week security
- But even simple CAPTCHAs represent a significant barrier for most primitive bots. We shouldn't deprive of it but please note that CAPTCHA does not protect you and/or your users about data/credentials leakage
- Although the main reason of using a captcha is to allow only humans to seek access but nowadays there are effective algorithms that allows bots to bypass the challenges easily
- Further we **can** also download browser extensions which solve the challenges on your behalf. **One** of them is Buster, which **does** a nice job in **bypassing** audio challenges, available with Chrome as well as Firefox. ... Instead of your human ear, the bot solves it for **you**.

Thank you!