CAPTCHA BREAKER
by

Priyanshu Parikh
Parth Rawal
Dhaval patel

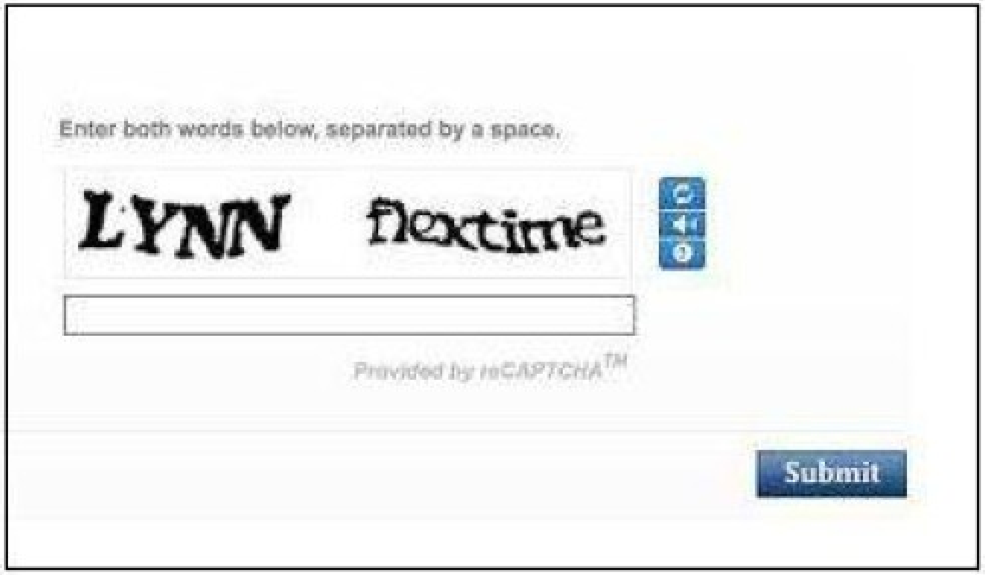
Internal Guide : Prof. Vishal Barot

Agenda

- Introduction
- Types of CAPTCHAs
- Preliminary Work Summary
- Our Approach
- Neural Networks
- Experiments
- Results
- Conclusion

Intoduction

- We are trying to decode CAPTCHAs using machine learning and deep learning.
- CAPTCHA: **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part.
- Helps to distinguish between humans and computers.
- First mentioned in a paper by Moni Naor [1] in 1996.



Enter both words below, separated by a space.

Provided by reCAPTCHA™

Characteristics of a CAPTCHA:

- Easy for a human to decode
- Difficult for a Computer to recognize.

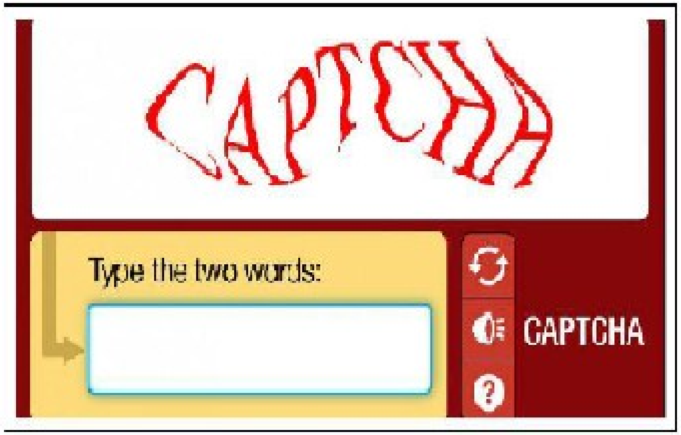
Why Decode CAPTCHAs??

- AI Problem
- Security Breach

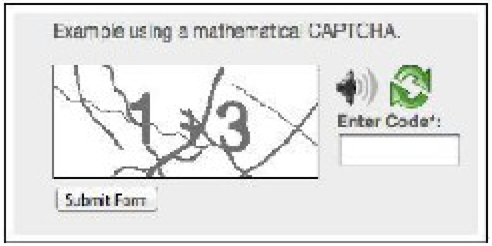
CAPTCHAs are critical for security on internet, if they are no more secure, our system won’t be secure and we would have to think of alternatives.

Types of CAPTCHAs

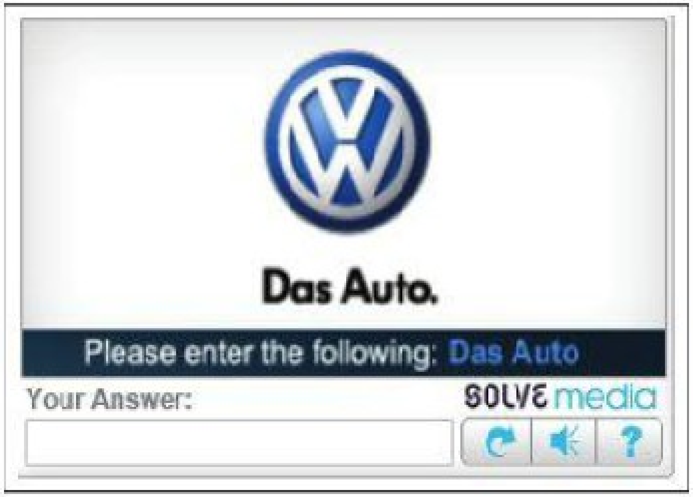
1. Standard Image Based CAPTCHA
2. Math Solution CAPTCHA
3. Picture Identification CAPTCHA
4. Ad-injected CAPTCHA
5. 3D CAPTCHA
6. jQuery sliderbar CAPTCHA
7. Drag and Drop CAPTCHA
8. Game CAPTCHA
9. reCAPTCHA



Type the two words:

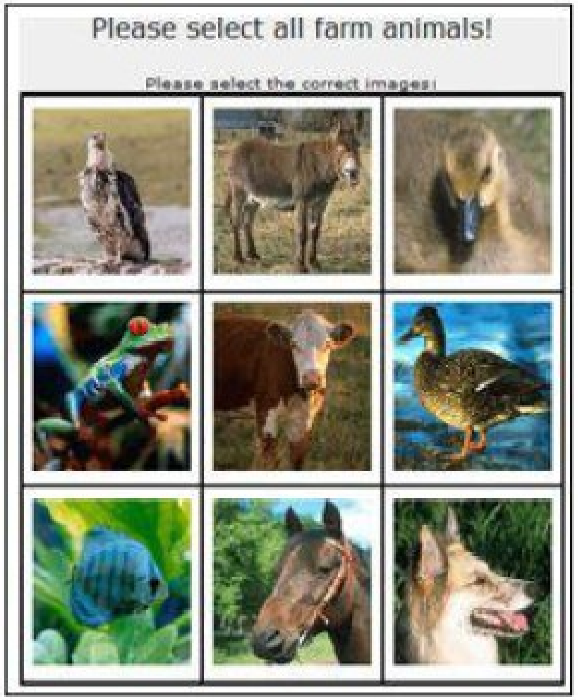

Example using a mathematical CAPTCHA.

Enter Code*:

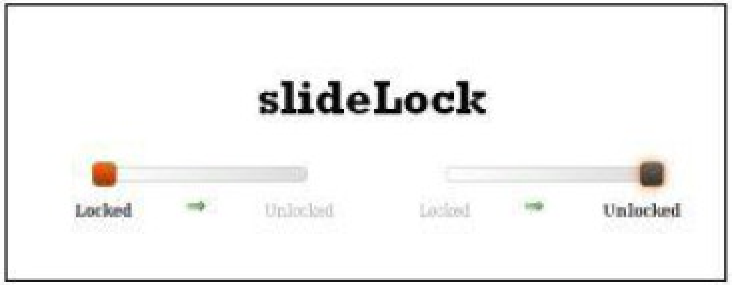


Please enter the following: Das Auto

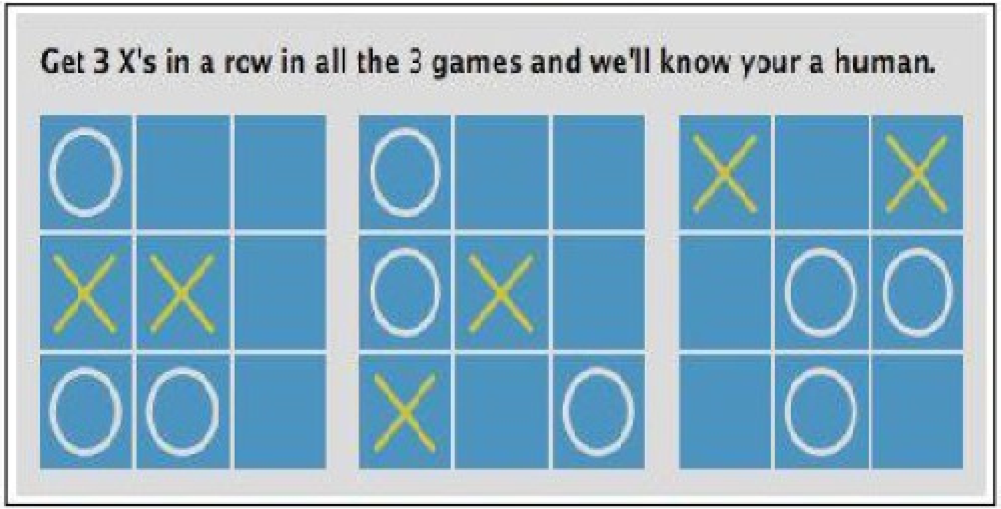
Your Answer:


Please select all farm animals!

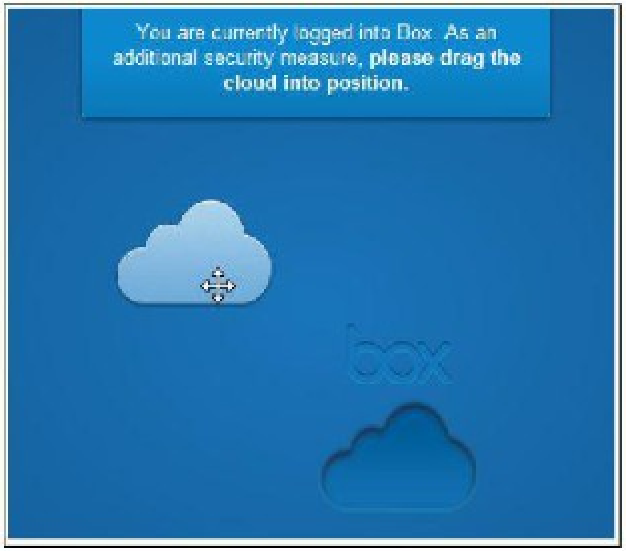
Please select the correct images:



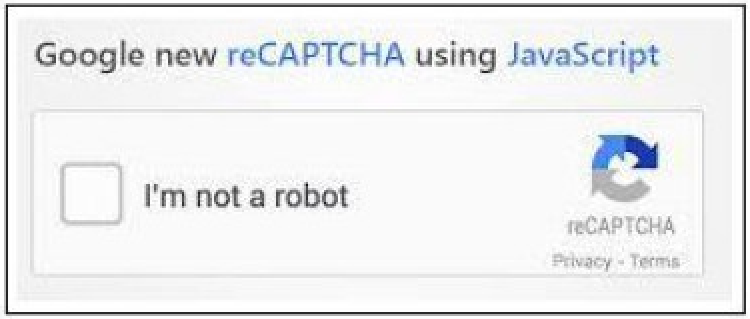
slideLock



Get 3 X's in a row in all the 3 games and we'll know your a human.



You are currently logged into Box. As an additional security measure, **please drag the cloud into position.**



Google new reCAPTCHA using JavaScript

☐ I'm not a robot

Preliminary Work Summary

- Breaking CAPTCHAs is not a new concept.
- Mori and Malik [2] have broken EZ-Gimpy (92% success) and Gimpy (33% success) CAPTCHAs with sophisticated object recognition algorithms.
- People [3] also have used the following approach for CAPTCHA recognition:
  - Preprocessing.
  - Segmentation.
  - Training the model for individual character recognition.
  - Generating sequence with highest probability

Our Approach

- Yann Le Cun used neural networks for handwritten digits
- recognition in 1990[6].
- Google has published a paper[4] in which they used convolutional neural networks to detect home addresses from street view home plate images.
- One more paper from Google[5] in which they used recurrent neural network to generate caption for an image.
- We will try combining these ideas !

Our Approach

- **End to End model.** Systems with multiple modules following conventional approach tend to behave poorly, because each module is optimized independently and the errors between modules compound. We learned an end to end model that predicts directly from pixels.
- **Convolutional neural network** for Image features and,
- **Recurrent neural networks** for generating output sequence.

Tools and Technology

- Python 3
- Pytesseract library
- OpenCV
- Keras
- Tensorlflow
- Optical Character Recognition(OCR)

Algorithms

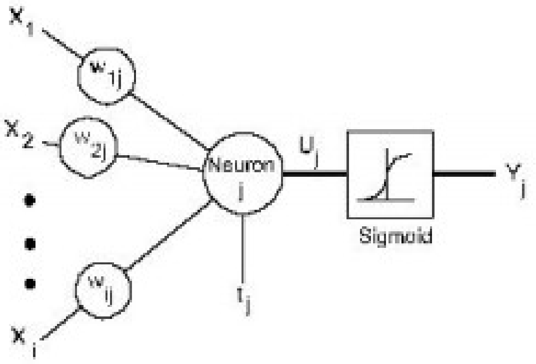
- Single Character Recognition
  1. Using Pytesseract
  2. k-means Clustering
  3. Support Vector machine (SVM)
  4. Convolutional Neural Network(CNN)
- Multi CAPTCHA Recognition
  1. Moving Window Algorithm
  2. Multi CNN Algorithm

Brief History of Neural Network

- Started way back in 1940’s.
- Became unpopular in 1960’s
- Regained popularity in 1980’s
- Recently have become one of the hottest areas in the field of machine learning.
- Applications involve face recognition used by Facebook,
- Image captioning used by Google etc

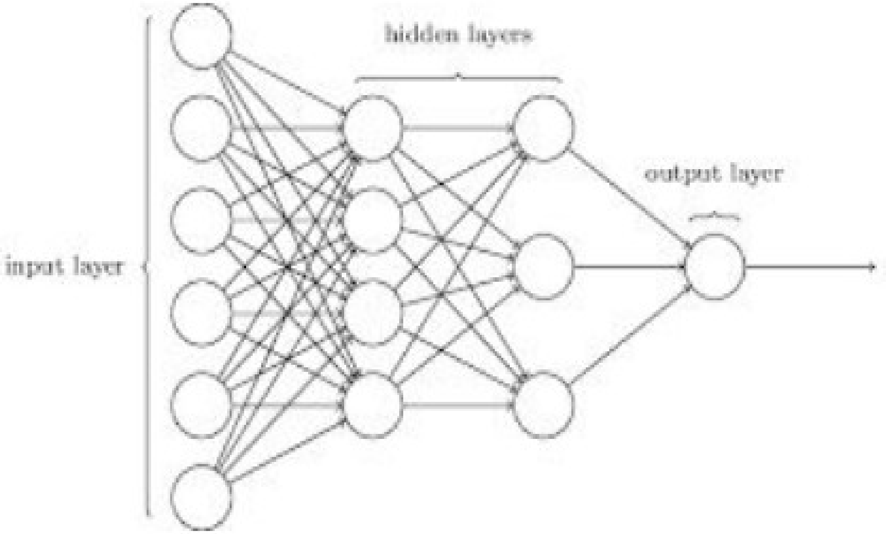
What are Neural Networks

- Inspired from human brain



A simple neural network model

- Many input units and one output unit.
- The inputs are scaled with weights on which an activation function is applied to get the output.



Multilayer neural network

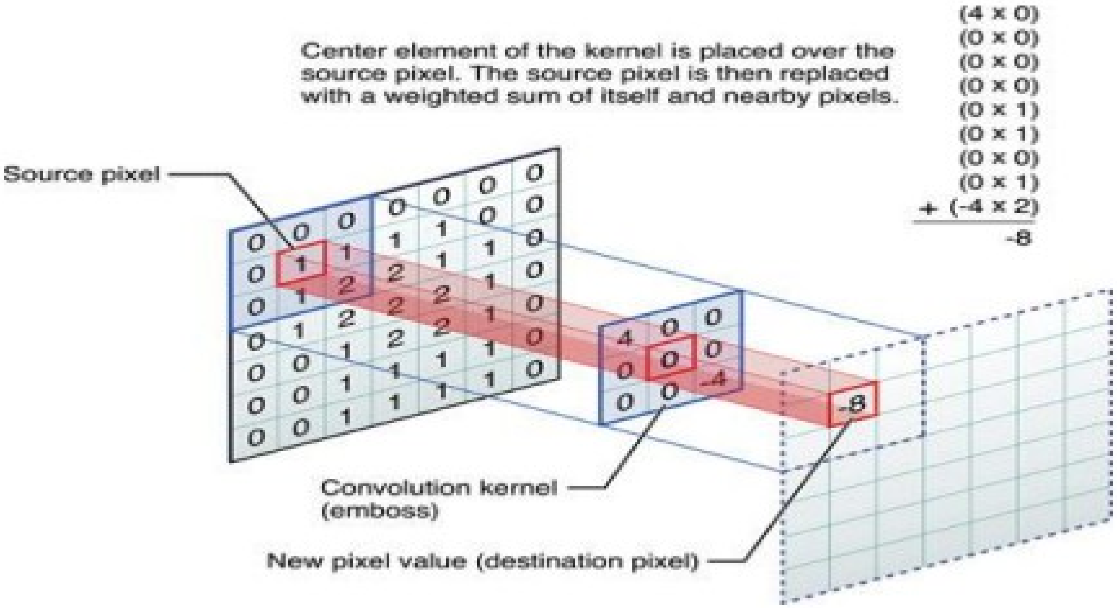
Training Neural Networks

- Backpropagation algorithm.
- The problem is set up as minimization of a loss (objective) function.
- Weights are adjusted using gradients and learning rate.
- Gradients are computed using simple derivative chain rule.

Convolutional Neural Network

- Convolutional Neural Networks are a special kind of multi-layer neural networks.
- In 1995, Yann LeCun Et al. introduced the concept of convolutional neural networks [7].
- Convolutional Neural Networks are designed to recognize visual patterns directly from pixel images with no preprocessing.

Convolutional layer



Center element of the kernel is placed over the source pixel. The source pixel is then replaced with a weighted sum of itself and nearby pixels.

(4 x 0)
(0 x 0)
(0 x 0)
(0 x 0)
(0 x 1)
(0 x 1)
(0 x 0)
(0 x 1)
+ (-4 x 2)
-8

Source pixel
4 0 0
0 0 0
0 0 -4
-8
Convolution kernel (emboss)
New pixel value (destination pixel)

Feature Extraction

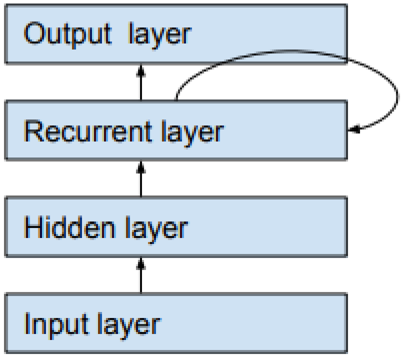
- Shared weights: The same filter weights are applied to all the pixels.
- It helps in detecting same feature at different locations of an image.
- This reduces the number of paramters to be learned.
- For Instance, if image size is 200*50, filter size is 5*5 and if there are 32 filters, we have only 32*(5*5 +1) (1 for bias) = 832 weights to learn.
- Otherwise it would have been number_of_pixels*number_of_pixels*filters, which would be 200*50*200*50*32 = 3.2 million.
- This is several orders of magnitude larger than what we have in CNNs.

Maxpool Layer

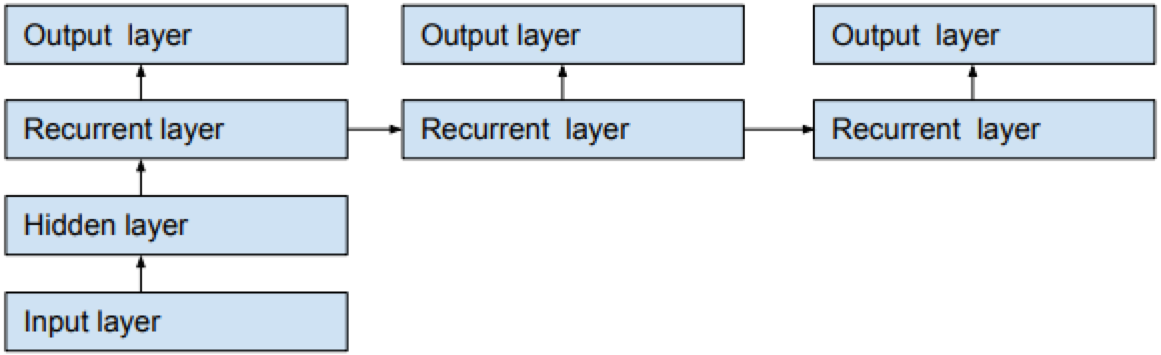
- Typically used after a CNN layer.
- Takes maximum of neighbouring pixels.
- Helps in rotational and translational invariance

Recurrent Neural Networks

- Feedforward networks accept only fixed sized input and give output of fixed length, whereas RNNs can work with variable length inputs and outputs.
- In RNNs, connections between units have a directed cycle.
- Various applications of RNNs include handwriting recognition and speech recognition.



RNN



RNN unrolled

Softmax Layer

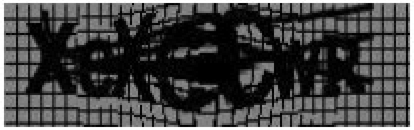
- Used for generating a probability distribution.
- Used typically in classification problems.
- In our model, we will use it to estimate probability of every character.

DATASET

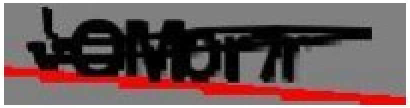
- We will use PyCaptcha, a python package for CAPTCHA generation, to make custom CAPTCHA image dataset.
- This package offers several degrees of freedom such as font style, distortion and noise, which we can exploit to increase the diversity of our data and the difficulty of the recognition task.

DATASET

- An image contains 4-7 characters, if it is variable length dataset or 5 characters if it is a fixed length captcha.
- A character could be A-Z, a-z or 0-9.
- All the images generated are of same size i.e. (200*50).



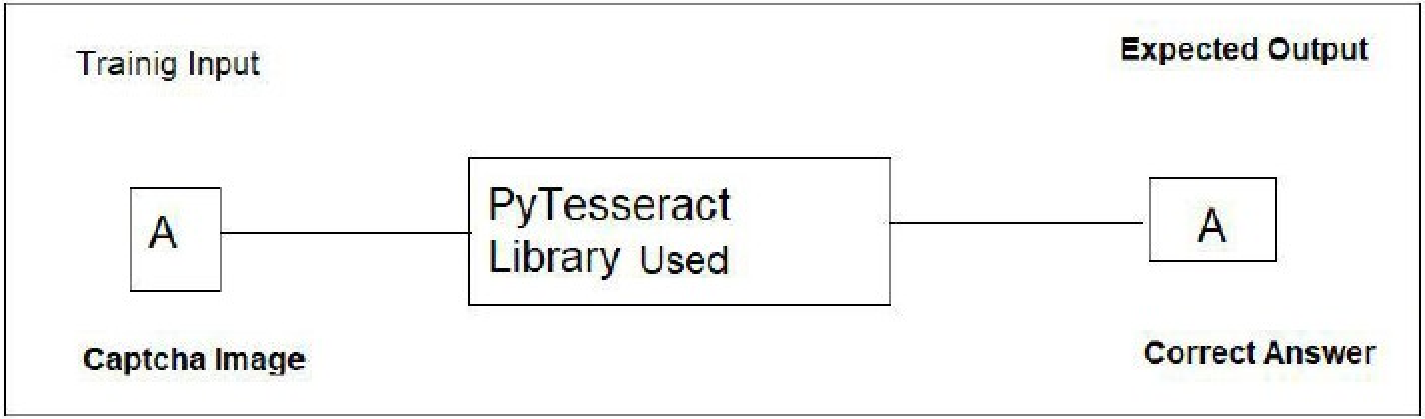
Complex image



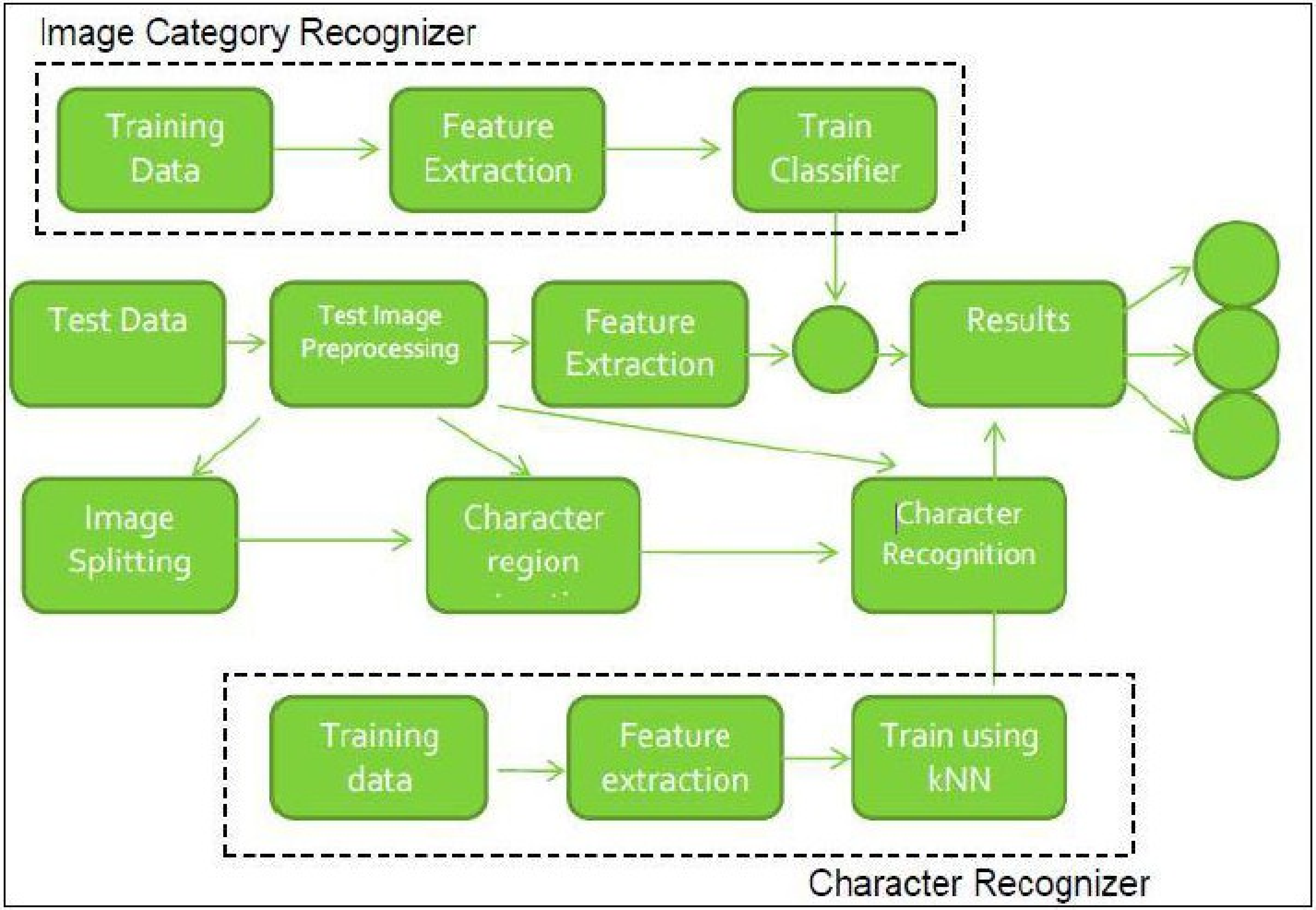
Simple Image

Experiments

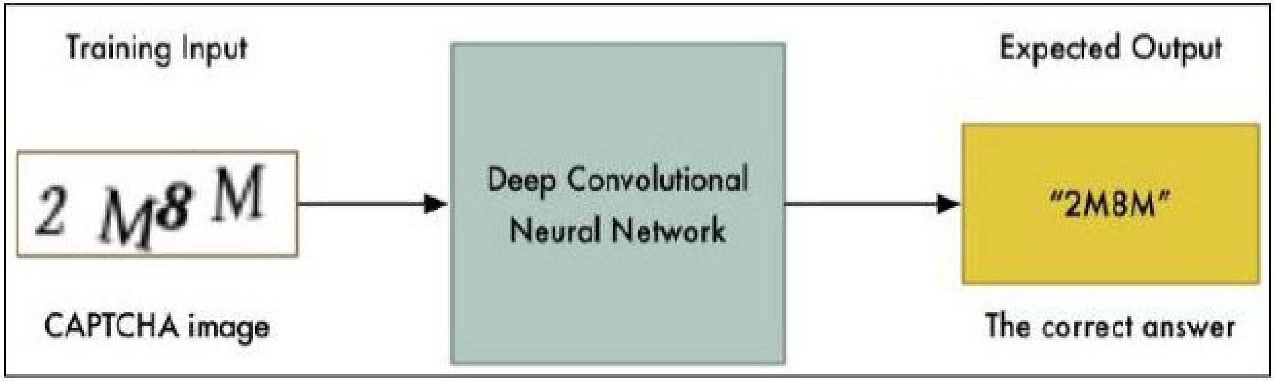
- Single Character Recognition

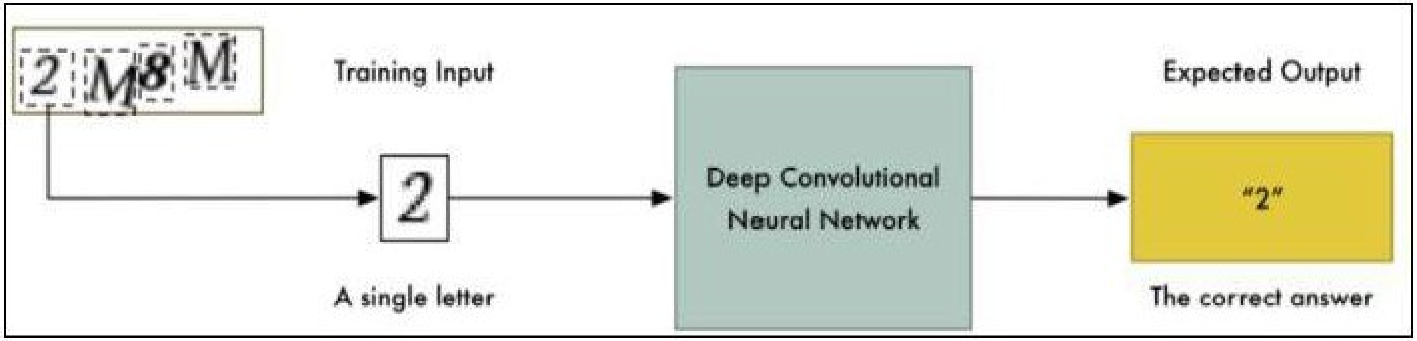


- K-means Clustering

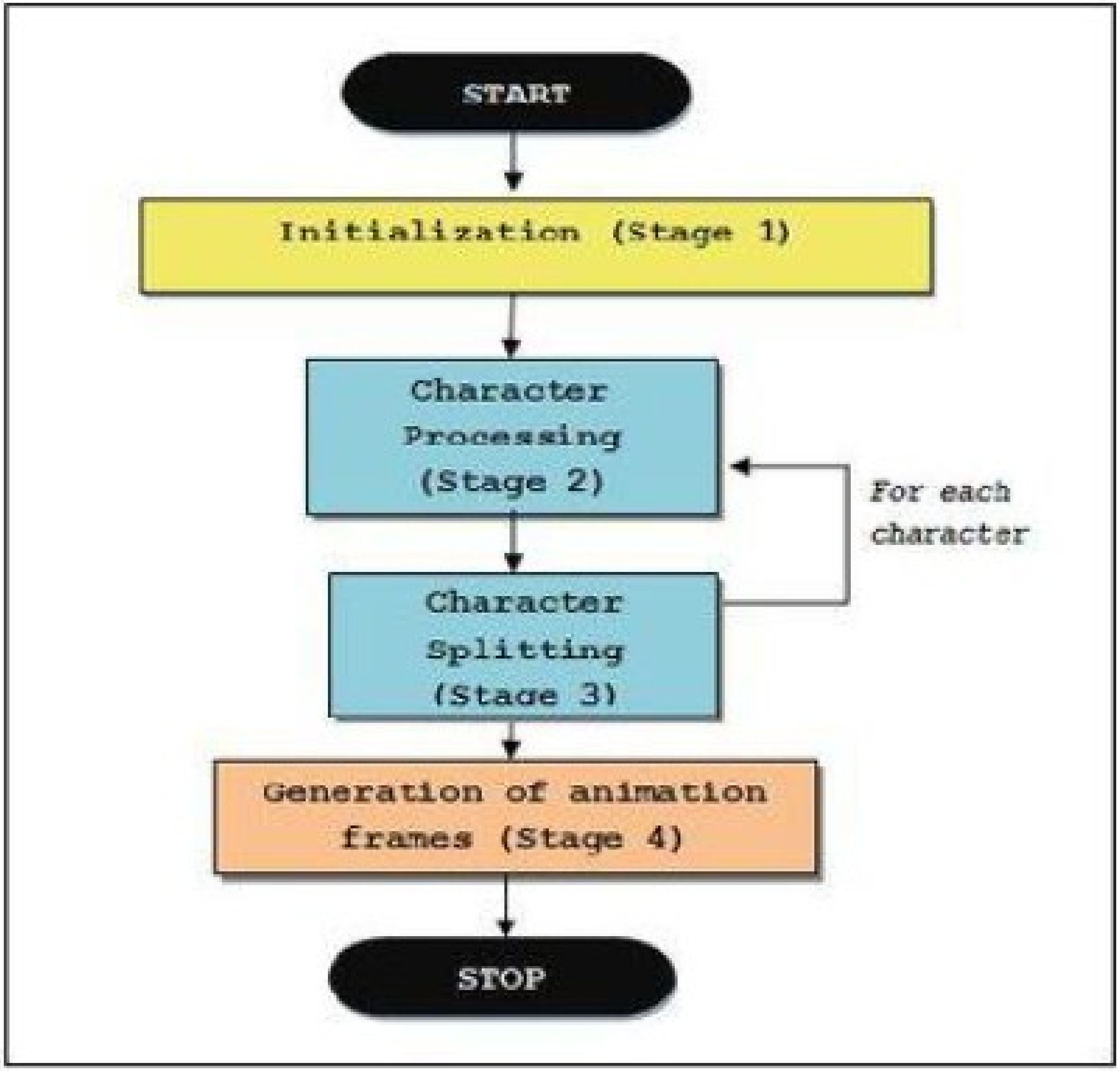


CNN

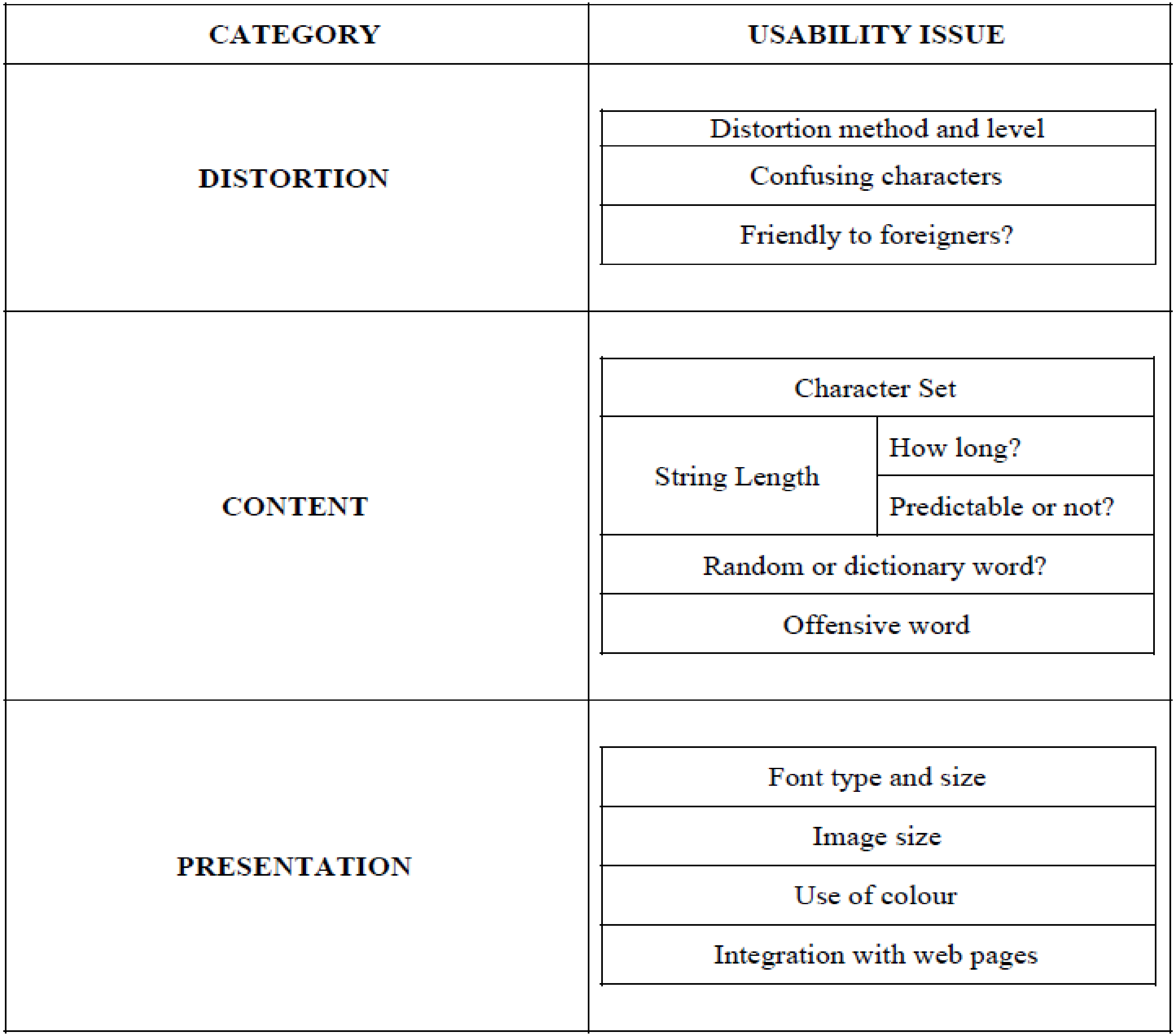

Training Input
2 M8 M
CAPTCHA image
Deep Convolutional Neural Network
Expected Output
"2M8M"
The correct answer


2 M8 M
Training Input
2
A single letter
Deep Convolutional Neural Network
Expected Output
"2"
The correct answer

FLOW CHART

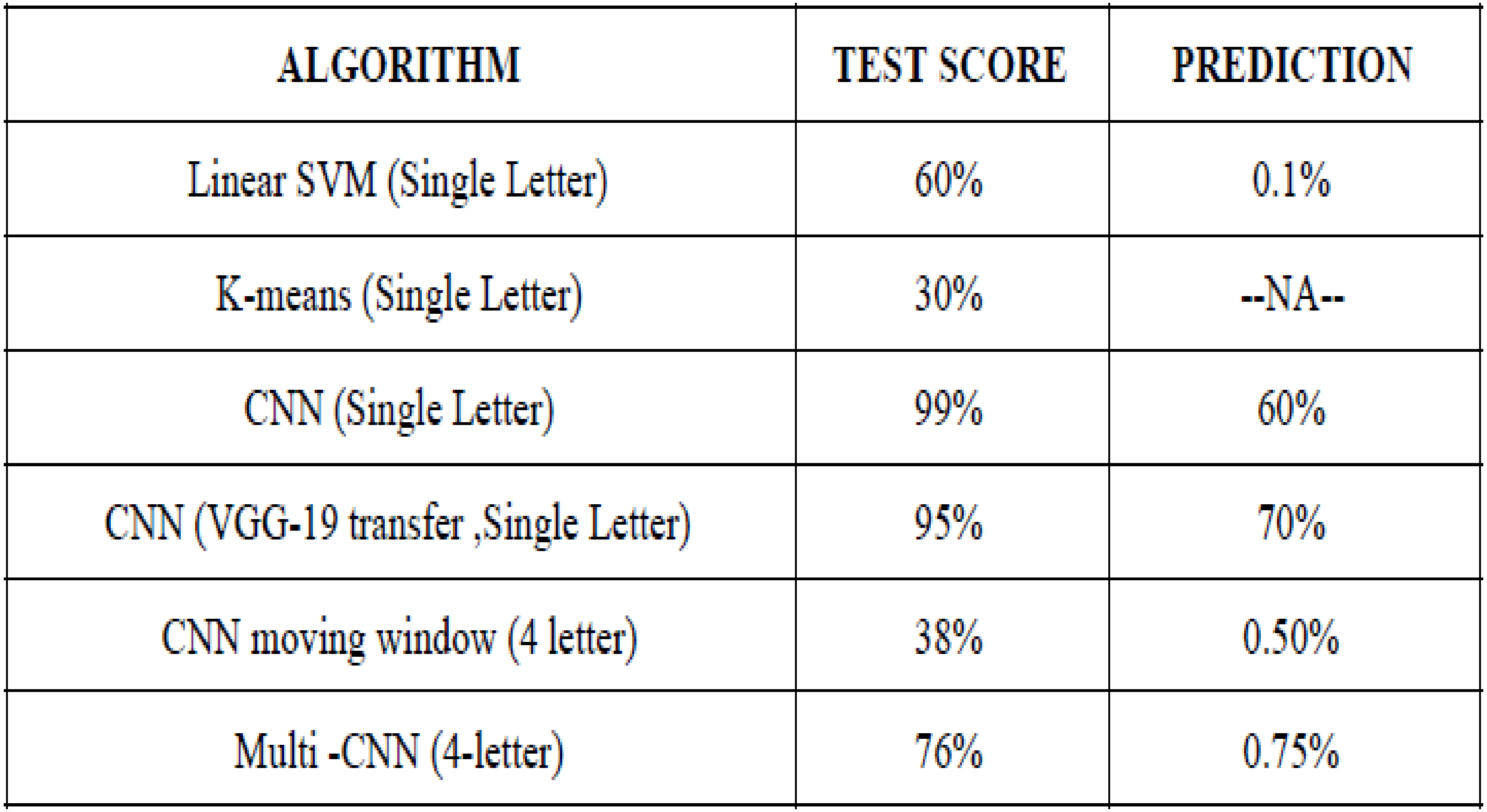

START
Initialization (Stage 1)
Character Processing (Stage 2)
For each character
Character Splitting (Stage 3)
Generation of animation frames (Stage 4)
STOP

ISSUES AND LIMITATION



CATEGORY	USABILITY ISSUE	
DISTORTION	Distortion method and level	
	Confusing characters	
	Friendly to foreigners?	
CONTENT	Character Set	
	String Length	How long?
		Predictable or not?
	Random or dictionary word?	
	Offensive word	
PRESENTATION	Font type and size	
	Image size	
	Use of colour	
	Integration with web pages	

Results



ALGORITHM	TEST SCORE	PREDICTION
Linear SVM (Single Letter)	60%	0.1%
K-means (Single Letter)	30%	--NA--
CNN (Single Letter)	99%	60%
CNN (VGG-19 transfer ,Single Letter)	95%	70%
CNN moving window (4 letter)	38%	0.50%
Multi -CNN (4-letter)	76%	0.75%

CONCLUSION

- Deep neural networks showed a really good performance in decoding CAPTCHAs with 80% and 99.8% accuracy for variable and fixed length CAPTCHAs respectively.

- CAPTCHAs are not more secure as computers can do better than humans.

Future Work

- Will try to work on accuracy using convolutional layers.
- Will make the system robust by increasing the variety in training data.
- For math solution CAPTCHAs we will implement Natural Language Processing Algorithms to our project and try to break that kind of CAPTCHAs.
- For identifying the Picture Based CAPTCHAs we will try for Google Reverse Image System that will identify similar kind of images that is given in the CAPTCHAs image and we will try to implement that algorithm to our project.

References

[1] Moni Naor. Verification of a human in the loop or Identification via the Turing Test. Unpublished Manuscript, 1997.

[2] Greg Mori and Jitendra Malik. Recognising Objects in Adversarial Clutter: Breaking a Visual CAPTCHA, IEEE Conference on Computer Vision and Pattern Recognition (CVPR'03), Vol 1, June 2003, pp.134-141.

[3] Kumar Chellapilla, Patrice Y. Simard Using Machine Learning to Break VisualHuman Interaction Proofs (HIPs) Microsoft Research, one microsoft way, WA 98052 -2005

[4] Ian J. Goodfellow, Yaroslav Bulatov, Julian Ibarz, Sacha Arnoud, Vinay Shet. Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks,14 Apr 2014.

[5] Oriol Vinyals, Alexander Toshev, Samy Bengio, Dumitru Erhan, Show and Tell: A Neural Image Caption Generator, 20 Apr 2015

[6] Y.Le Cun Et. al. Handwriting Character Recognition using Neural Network Architecture.1990

[7] Y. LeCun and Y. Bengio. Convolutional networks for images, speech, and time-series. In M. A. Arbib, editor, The Handbook of Brain Theory and Neural Networks. MIT Press, 1995.

THANK YOU!!