Recognition of Text CAPTCHA by using Back Propagation Algorithm of Artificial Neural network

Sumeet Gill, Renu Saroha

Abstract: Text-based CAPTCHA is a very simple type of CAPTCHA which are most widely used. It uses only a group of characters. In this paper, we focus on how Text based CAPTCHA is recognized by machine learning techniques. This paper proposed a method based on Back Propagation algorithm to identify the Text based CAPTCHA. The proposed technique improves the security level of Text-based CAPTCHA storage system by using the Back-propagation method of Artificial Neural Network. We used NNToolbox to train the network in MATLAB software.

Keywords: Text-based CAPTCHA, Back-propagation Algorithm, Artificial Neural Networks.

INTRODUCTION:

Now a days, all work is mostly done on the internet like education, shopping, net banking, and social discussion. On the majority of these sites, users need to fill their registration form by entering all the personal information in order to surf that particulars sites and different kinds of other survey forms. Due to increased technology, hacking software are available to fill all details automatically. One of the most important fields in our modern technology is related to protecting the information and securing it. The term CAPTCHA was invented by Luis Von Ahn, Manuel Blum, Nicholas J, Hopper and John Langford at Carnegie Mellon University (CMU) in 2000 [1]. CAPTCHA is an important standard internet security technique to protect e-mail and other services from bots attack. It is successfully applied a number of application domains including education, business, social sites, and etc. CAPTCHA is "Completely automated public Turing test". Turing test is the standard interpretation of the behaviour of a machine in certain fixed options where the machine is to make decisions based on the inputs presented to it [2]. A good example of standard interpretation is as follows:

Suppose we have three players A, B, and C. Player C is the interrogator, who has given the test of guessing which player (player A or Player B) is a computer and which is human. Automated means to quickly perform the measurement and evaluate the test result. Turing test is for the standard interpretation of the behaviour of a machine in a certain fixed option where the machine is to make the decision based on the inputs presented to it. It is a security test that differentiates a computer and human apart. CAPTCHA code is a new network security technology. This technology is related to the protection of information and provides a way of securing it. It is also known as human interactive proof system that is used to secure our application on the internet. The normal scenario for providing protection and security against attacks is to use unique username and password, but this kind of security is normally breached and various attacks are being performed by different programs and various software are used for applying automatic attacks. CAPTCHA prevents the entry of automated script known as Bots. Bots are usually a robot which replicates the behaviour of humans and carries out malicious activities on web applications. Internet bots are also known as a web robot. It is a software application that runs automated tasks over the internet. The main advantage of CAPTCHA is that it is difficult for computers to extract the texts form such as distorted or puzzled images whereas it is easy for humans to understand the text hidden behind the distortion. Text-Based CAPTCHAs are randomly generated and are very simple to implement. It is a very effective technique and requires a large question bank. Text CAPTCHAs are displayed to the user during the signing up process. Text-based CAPTCHA includes simple type of question like, What is 5+4=? , What is 6*7=?, Which one among apple, curd, table, pen is fruit?, Enter the number thirteen, hundred forty-three?, How many colors are there in a rainbow?, Which is 2nd in the series 35,19 and thirty-four?, Which one among socks, library, cake or red is a colours? Text-based CAPTCHA is seen at the bottom of any application and registration form. CAPTCHAs faces a lot of problems like brute force attacks, relay attacks, dictionary attacks, denial-of-service attacks and, etc. Text-based CAPTCHAs are easily recognized by OCR (Optical Character Recognition). These are easy for a tester machine to generate and grade but hard for a software robot to pass.

As studied in previous year papers, to recognize the text Convolution Neural Network algorithm is used [8]. This algorithm includes three steps to recognize, these are: pre-processing, segmentation and recognition of images. In this paper, the Back propagation algorithm is used and it does not require pre-processing, segmentation and recognition of images. It

Revised Manuscript Received on July 22, 2019.
    Sumeet Gill, Associate Professor in Department of Mathematics, Maharshi Dayan and University, Rohtak-124001, Haryana (India)
    Renu Saroha, Ph.d Scholar Department of Computer Science Application, Maharshi Dayan and University, Rohtak-124001, Haryana (India)

takes more time but here we don't require any further steps to recognize the characters.

Images of Text-Based CAPTCHAs

~~Zitgg~~	jqqan	*Zilgh*	<u>*DzyHn*</u>	Fyval
Ggt3f	Tyve2	Halt2	Qqu3i	
Of6th	Pulot	3Wnliq	*Mqu45*	Taqu4
Othis	roscoe	Jb4n2	~~emper~~	Senec

Different 10-bit input pattern say $(x_1, x_2, x_3, x_4 \text{-------} x_{10})$ and observed 10- bit output pattern say $x_1, x_2, x_3, x_4 \text{----} x_{10})$.

Input Layer	Hidden Layer	Output Layer

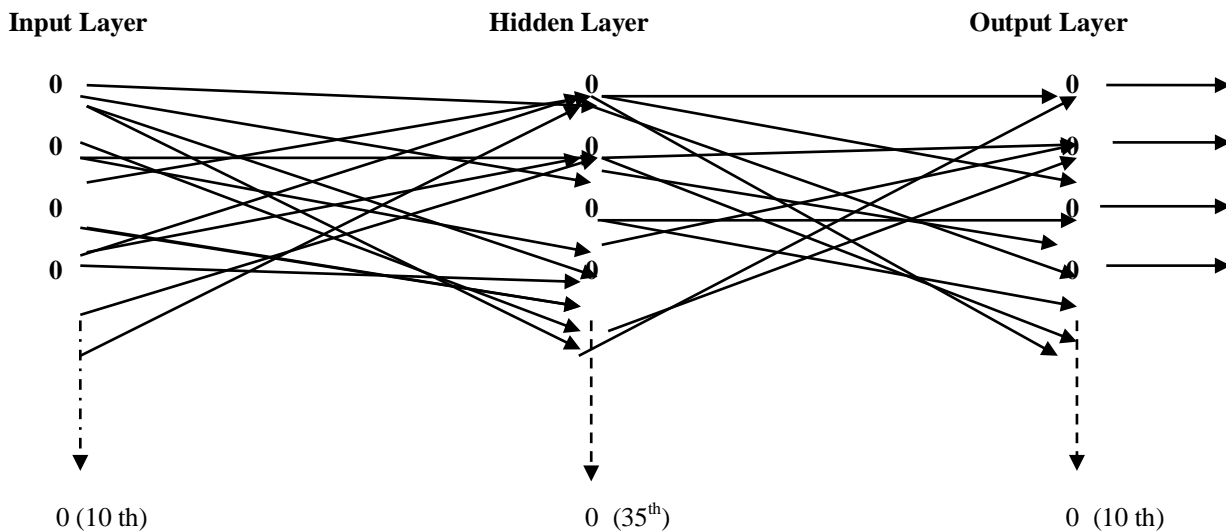| 0 (10 th)	0 (35th)	0 (10 th)

Figure1 Shows Neural Network Architecture for a Feed Forward Network

The input and output values of the network are represented as S_i and S_o. The activation output information for the input layer is x_i and for the output layer is y_j . The output activation for the hidden layer is S_h and q_h. The output signal and the activation values for the input, hidden and output layer are represent as for the 1th pattern in mth iteration.

Experimental Design

In this experiment, we are performing the actual training and experiment conducted on dummy data. Here we memorize the input pattern sets by minimizing the error between the as training data set desired and actual output for the 10 input set and 10 output set. The last 40 bits are being used as test patterns. In this experiment, we estimate the password storage with standard Back Propagation Model. The experiment described is designed to achieve the encryption pattern storage in the network. The experiment has been conducted in MATLAB 2016.

The initial parameters taken before training for formation on network are given in table below:

Parameters	Value
Neurons in input layer	10
Number of hidden layers	1
Neurons in hidden layer	1

1449

Neurons in output layer	10
Minimum error exist in the Network	0.001
Initial Weights and biased term values	Values between 0 and 1

Table1 : Parameters used for Training of Network using Back Propagation Model

Input pattern sets

Training of the system was carried out for following 10 input pattern sets:

1	1	1	1	1	1	1	0	1	1
0	0	0	0	0	0	1	1	1	1
1	0	1	0	0	0	0	0	0	0
1	1	1	0	0	0	1	0	1	1
0	0	0	1	1	1	0	0	1	0
1	1	1	0	1	1	1	0	1	0
0	0	0	0	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	1	0	1	1
0	1	0	1	1	1	0	0	1	0
1	0	1	1	0	0	0	1	1	1
0	0	0	0	1	1	0	0	0	1
1	0	1	1	1	1	1	0	0	1
0	1	0	0	0	0	0	1	0	1
1	1	1	1	1	1	1	1	0	1
0	0	0	0	0	0	1	0	1	1
1	1	0	1	0	0	1	1	1	1
0	0	1	1	0	0	1	0	0	0
1	0	1	0	0	1	0	1	0	0
0	0	0	0	0	0	0	0	1	0
0	1	0	1	1	0	0	0	1	0
1	1	1	1	1	1	1	1	0	1
0	0	0	0	0	0	1	0	1	1
0	0	0	0	1	1	0	1	0	0
0	0	0	1	1	1	1	0	1	1
1	0	1	0	0	0	1	1	0	0
1	1	1	0	0	1	0	0	0	0
1	1	1	0	1	0	1	1	1	1
1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	1	0	1	1
0	0	1	0	0	1	0	0	0	0
0	1	1	1	1	1	1	0	1	0
1	1	0	1	1	0	0	1	0	1
1	1	1	1	0	1	0	1	1	0
1	0	0	0	0	0	1	0	0	1

Table2. Shows Input pattern dataset sets

Test Pattern Sets

The following pattern sets were chosen to be test patterns for recalling:

1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	0	1	0
0	0	0	0	0	0	1	0	0	1
0	1	1	1	1	1	0	1	1	1

Determining of Coupling Strength between the Neuron Layers.

Recognition of Text CAPTCHA by using Back Propagation Algorithm of Artificial Neural network

For estimating the training of encryption pattern of passwords, we first need to define the functional dependency between the encrypted passwords in the form of weights in the neural network.

Between Input Layer to Hidden Layer			Initial Weights		
0.39483	-0.34012	-0.61717	0.40563	0.48655	-0.27982
-0.22963	-0.46503	0.28964	-0.30761;	-0.22963	-0.46503
0.36838	0.59305	0.14725	0.45316	-0.16646	-0.35268
0.51488	-0.19476	-0.17803	0.01263	-0.17999	-0.21126
0.39483	-0.34012	-0.61717	0.40563	0.48655	-0.27982
-0.30761	-0.22963	0.28964	-0.30761;	-0.46503	0.28964
0.36838	0.59305	0.14725	0.45316	-0.16646	-0.35268

0.33097	-0.43069	-0.41724	-0.048845	-0.26455	-0.45947
0.53351;	-0.13582	-0.43691	-0.065149	0.22913	-0.042134
-0.090708	0.317	0.28739	-0.52859	-0.43479	0.2426;
0.42716	0.44417	0.081215	-0.42247	-0.11168	-0.1049
-0.40321	-0.28442	-0.029918	-0.61638	-0.12866	-0.28887
0.33097	-0.43069	-0.41724	-0.048845	-0.26455	-0.45947

Table4. Shows the weights matrix of Test pattern sets.

Results

Memorised Pattern Set

The network was trained for following 10 input output pattern sets.

1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1	1
2	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	1	1	1	1
3	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0
4	1	1	1	0	0	0	1	0	1	1	1	1	1	0	0	0	1	0	1	1
5	0	0	0	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1	0
6	1	1	1	0	1	1	1	0	1	0	1	1	0	1	1	1	0	1	0	
7	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	1		1	1

10	0	1	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	1	0
11	1	0	1	1	0	0	0	1	1	1	1	0	1	1	0	0	0	1	1	1
12	0	0	0	0	1	1	0	0	0	1	0	0	0	0	1	1	0	0	0	1
13	1	0	1	1	1	1	1	0	0	1	1	0	1	1	1	1	1	0	0	1
14	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0	1
15	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1
16	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	1	1
17	1	1	0	1	0	0	1	1	1	1	1	0	1	0	0	1	1	1	1	1
18	0	0	1	1	0	0	1	0	0	0	0	0	1	1	0	0	1	0	0	0
19	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0	1	0	1	0	0
20	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0
21	0	1	0	1	1	0	0	0	1	0	0	1	0	1	1	0	0	0	1	0
22	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0	1
23	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	1	1
24	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	1	0	1	0	0
25	0	0	0	1	1	1	1	0	1	1	0	0	0	1	1	1	1	0	1	1
26	1	0	1	0	0	0	1	1	0	0	1	0	1	0	0	0	1	1	0	0
27	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1	0	0	0	0
28	1	1	1	0	1	0	1	1	1	1	1	1	1	0	1	0	1	1	1	1
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	1	0	1	1
31	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0
32	0	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	0	1	0
33	1	1	0	1	1	0	0	1	0	1	1	1	0	1	1	0	0	1	0	1
34	1	1	1	1	0	1	0	1	1	0	1	1	1	1	0	1	0	1	1	0
35	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	1	0	0	1

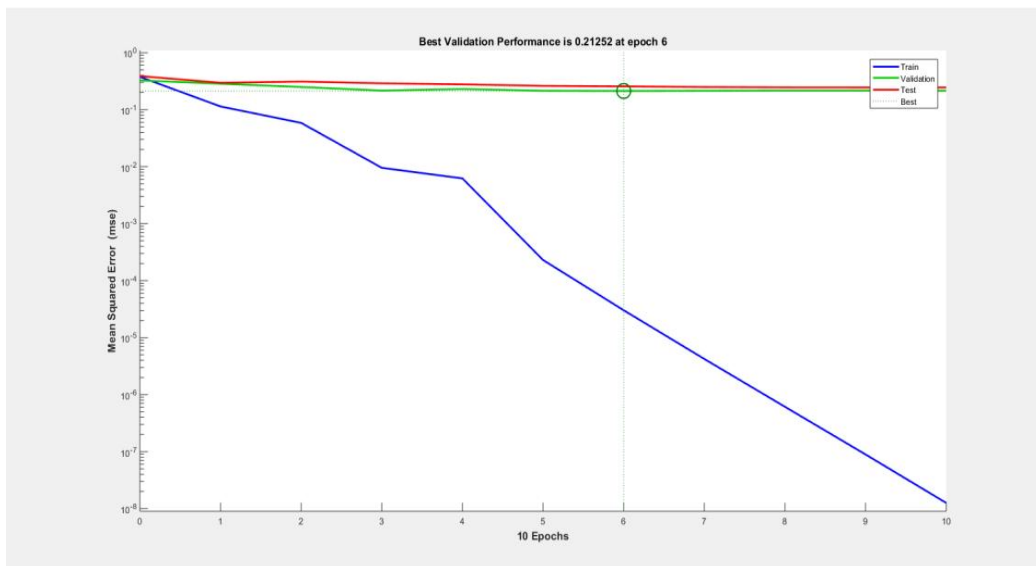**Table 4--- Memorised Pattern Set for Feed Forward Network trained by Back Propagation**

Figure2 . Shows The Performance Curve of Neural Network

Validation by Test Pattern :

The network was successfully trained and when we fed the test patterns, the result so obtained are shown in table below.

Test Pattern

Recognition of Text CAPTCHA by using Back Propagation Algorithm of Artificial Neural network

1	0	0	0	0	0	0	1	0	1
0	0	1	0	0	1	1	0	1	0
0	0	0	0	0	0	1	0	0	1
0	1	1	1	1	1	0	1	1	1

Output for Test Pattern (bit by bit) By the Network.

0.86393	0.17279	0.81072	-0.95569	-0.92987	-0.89381
0.89422	-0.74509	-0.94759	-0.82977	-0.76931	-0.17444
-0.39197	0.94074	0.83381	0.94886	0.92379	0.8375
-0.12771	0.24354	0.29411	0.92561	-0.81538	-0.30699
-0.26994	-0.036851	0.16146	0.20129	-0.32514	-0.34186
-0.26994	-0.036851	0.16146	0.20129	-0.32514	-0.34186
0.34985	-0.90363	-0.21114	-0.38456	0.39822	-0.38826
-0.1756	-0.17135	-0.20477	0.13256	0.15689	-0.058926
0.052763	0.82731	-0.065994	-0.83008	0.15434	0.127
-0.30175	0.38736	0.052211	0.070218	-0.0083134	-0.40444
-0.32589	-0.19489	0.0052044	0.026907	-0.93278	0.35184
0.90919	-0.31459	0.2593	-0.28413	-0.91	0.33599
0.21378	-0.025403	0.26298	-0.00509	-0.39976	-0.8233
0.73362	0.27761	-0.35748	-0.032807	0.11863	0.038341
0.075215	-0.15065	0.37533	0.3742	-0.32951	0.3084
-0.38729	0.9328	0.020015	-0.090406	0.20527	-0.1821
0.37804	-0.91504	0.18206	0.2553	-0.32821	0.25141
0.15471	-0.21882	-0.21357	-0.069184	0.80712	0.90215
-0.21752	0.15662	0.17986	0.073244	0.34196	-0.21752
-0.18171	-0.15355	-0.90093	0.83037	0.094684	0.14227
-0.094379	-0.16688	0.022904	0.12374	-0.37663	0.36544
0.80574	0.29664	-0.0085408	0.17461	0.32188	0.80092
0.20103	0.02024	-0.31115	-0.2894	0.08821	-0.32378

-0.036538	-0.27211	0.02103	-0.92587	-0.057359	0.077398
0.34303	0.93417	0.2084	-0.33183	-0.39826	0.14368
-0.11019	-0.80139	-0.18409	0.2271	0.21161	0.17593
0.2143	-0.18331	0.28035	0.26513	-0.31871	-0.24507
-0.27264	-0.36816	-0.13653	-0.34782	-0.056755	0.026235
-0.25473	0.22406	0.054299	0.079148	-0.97791	-0.18663
-0.15125	-0.31519	-0.0131	0.94957	0.36588	-0.14673
-0.045166	-0.085953	-0.068903	-0.20416	-0.30334	-0.32353
-0.2958	0.30919	0.93587	0.81712	0.074728	-0.037872
-0.33472	-0.23202	0.12405	-0.1536	0.15476	0.22397
0.38411	0.039047	-0.11226	0.5011	-0.041316	-0.11629
0.045994	-0.17944	-0.35453	-0.03003	-0.09832	0.39248
0.12324	-0.32306	0.077038	-0.1627	0.31153	-0.29617
0.47252	-0.18373	0.026629	0.27935	-0.3734	-0.38674
-0.056507	-0.32645	0.47965	-0.015406	0.13766	0.14539
0.39748	-0.94506	0.23669	-0.12832	0.25321	0.12927
0.9192	0.87369	0.91252	-0.32134	-0.94723	-0.22002
-0.31483	-0.31017	-0.039011	-0.026245	0.098319	-0.35762
0.25676	-0.24953	-0.24072	0.1821	0.046442	0.20381
0.17207	0.33167	-0.95766	0.31598	-0.076024	-0.43502
0.16071	0.0049736	-0.3621	0.16954	-0.061718	-0.34223
-0.089626	-0.23779	-0.29253	0.90588	-0.80646	-0.21171
-0.1422	0.26198	-0.33945	-0.3657	-0.056139	-0.035928
-0.26383	-0.30569	-0.14013	0.31039	-0.28046	0.32772
-0.90531	-0.043533	-0.38101	-0.1229	0.92769	0.31905
-0.25371	-0.2567	0.29877	-0.027529	0.22824	-0.32488
0.085509	0.13576	-0.31928	0.10535	0.2304	0.055341
-0.064298	0.26273	0.40254	-0.17709	0.93413	-0.064298

-0.8401	0.14963	0.82339	0.13571	-0.8401	0.14963
0.072292	0.016923	-0.30386	-0.038694	0.049022	0.91992
-0.089454	0.22156	0.013522	0.10553	-0.089454	0.12287
-0.94948	0.91227	-0.10376	0.21526	0.25781	-0.94948
0.35975	-0.096596	0.24154	0.37091	0.041005	0.38636
0.21382	0.01629	0.36824	-0.10839	-0.35548	0.38864
0.19427	0.14187	-0.045229	-0.092243	0.33666	0.92923
-0.31361	-0.10395	0.21082	0.37117;	0.94455	-0.31361
0.25819	0.30561	-0.18357	-0.30937	0.25819	0.30561
0.11379	-0.36613	0.31021	-0.28586	-0.30391	0.32259
-0.25118	-0.012844	-0.067866	0.020552	2.1816e	-005 0.459
-0.93498	-0.30055	0.095804	0.13391	-0.025782	0.26283
0.23696	0.14946	-0.015458	0.31202	0.23696	0.21156
0.27109	0.030159	-0.24966	-0.10156	-0.067796	-0.33314
-0.2837	-0.021222	0.15748	0.25141	-0.075835	-0.030733
0.98377	-0.36707	-0.15832	0.27852	0.21567	-0.36492
-0.021643	0.12125	-0.37836	-0.057049	0.24973	0.29304
0.316	-0.32205	-0.93689	-0.24714	-0.32106	0.27282
0.95726;	0.28701	-0.29929	0.91029	-0.31957	-0.33879
-0.38571	-0.050864	0.38698	-0.010612	0.38683	0.28706
-0.22068	-0.017183	0.18729	-0.24783	-0.15185	0.15485
0.12224	-0.055144	-0.28687	0.28803	-0.13151	-0.3188
-0.42606	0.059127	0.38723	0.22398	0.25991	0.28467
-0.17445	0.35471	0.17354	-0.32161;	-0.36658	-0.010478
-0.15356	0.10439	-0.37253	-0.37672	-0.19823	0.99109
0.12699	0.11246	-0.047294	-0.078988	-0.38835	0.20461
0.18028	0.10993	-0.085823	0.27841	-0.99178	-0.095244
-0.27859	-0.46111	0.12382	-0.33052	-0.32327	0.03457
-0.45927	-0.30128	-0.012689	-0.18791	-0.15275	-0.037608

0.83105	-0.089213	-0.062046	-0.34596	-0.27027	0.92109
0.50405	0.0097021	-0.069704	0.20426	0.13417	-0.077091
0.054585	0.10206	0.15796	-0.24052	-0.35149	0.38989
0.99357	-0.19287	0.28359	-0.002173	-0.011893	0.084048
0.18564	0.11085	-0.44567	-0.98702	-0.1274	0.30668
0.37267	0.13116	-0.22313	0.13812	0.071448	0.40888
0.0096557	-0.34859	-0.093661	0.32221	0.29161	0.39687
-0.24545	-0.91808	0.15401	0.21373	0.29843	0.42377
-0.067849	0.29185	0.35933	-0.27564	-0.90152	-0.15165
-0.17934	0.29206	-0.36885	0.046415	-0.09322	-0.22317
-0.18453	-0.35989	0.069377	0.29509	0.21143	0.11719
0.19108	0.050353	0.075952	0.32077	-0.24433	-0.13387
0.30851	-0.92065	-0.083069	-0.11652	-0.83545	0.19707
-0.25969	-0.24597	-0.31101	-0.232	0.98746	0.29283
-0.38064	0.93546	0.90242	-0.36949	-0.1635	0.3013
-0.27372	-0.2293	0.3968	-0.50052	0.030932	0.32677
0.39201	0.21728	-0.022788	0.21171	-0.3029	0.2836
0.25153	-0.077874	0.41631	0.065454	-0.31295	0.41211
0.070798	-0.15391	-0.36856	0.35612	0.096797	-0.30809
-0.25845	-0.15482	0.29448	-0.25125	0.19508	-0.32576
-0.24519	-0.17577	0.37795	0.12109	-0.3948	0.17338
0.15617	-0.287	-0.27726	-0.20679	0.16853	-0.24237
-0.34312	-0.35344	-0.21485	-0.26858	0.033399	-0.26535
-0.24991	0.089004	0.21239	0.34814	0.036862	0.25824
-0.38252	0.25738	0.52853	0.92738	0.26654	0.1988
-0.016794	0.18753	0.060316	0.1055	0.38203	-0.36406
-0.441	0.10269	0.17069	0.31423	-0.3953	0.11593
-0.1153	-0.22586	0.36585	-0.24702	-0.10359	0.19101

Retrieval Number: I33080789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3308.0789S319

1456

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

-0.19905	0.1467	-0.05352	-0.26212	0.25218	0.038696
-0.066563	-0.38948	0.081674	-0.29533	-0.9147	0.037977
-0.80705	-0.9651	-0.34946	-0.33069	-0.066902	-0.29974
-0.15643	0.15766	-0.25772	0.32268	0.14335	0.078804
-0.25049	-0.13776	0.29686	0.28797	0.095051	0.38197
0.35723	0.30627	0.15374	0.10822	-0.085382	0.15512
-0.28775	0.34191	0.02348	0.35839	-0.35888	-0.23408
-0.4227	0.33313	0.19124	-0.238	-0.34089	-0.91734
0.26057	-0.044604	-0.26615	-0.18556	0.36451	-0.90279
0.39092	-0.3039	0.044788	0.37231	0.011934	-0.9365
0.029567	0.19025	0.26678	-0.82454	0.27325	0.035243
-0.21142	0.28822	0.31021	-0.19141	-0.21187	0.027332
-0.098016	-0.32761	0.1499	0.21178	0.12178	0.39129
-0.90195	0.15125	-0.35097	-0.35975	0.098953	-0.3807
-0.042702	0.014915	0.24079	0.16175	-0.34479	0.37754
-0.31458	-0.08886	-0.91355	-0.13509	-0.25181	-0.36315
-0.0091389	-0.39776	0.17928	0.29355	0.19761	-0.14076
-0.37003	-0.16464	0.32682	0.24354	0.16167	-0.37693
-0.1974	0.93836	-0.19199	-0.052739	0.093635	-0.34615
-0.18636	-0.39872	0.37447	-0.070003	0.18344	0.15493
0.25363	-0.0016099	-0.21075	0.32063	-0.91728	-0.32574
0.93201	-0.37649	-0.23433	-0.32678	-0.099137	0.16387
0.97497	0.86118	0.27605	0.074995	-0.37472	-0.014905
-0.10156	-0.0047461	0.12395	0.037982	0.35322	-0.084116
-0.97896	0.025687	0.13848	-0.25844	-0.18125	0.20342
0.25555	0.98322	0.27033	0.0403	-0.13816	-0.27336
0.39514	-0.21371	-0.17305	0.50312	0.028248	-0.3383
0.24201	0.032934	0.18429	0.19273	0.96229	-0.11198
0.32427	-0.32613	0.16916	0.20513	0.30014	-0.036955

0.91747	0.24144	-0.17993	0.032449	0.28665	0.91747
0.06074	0.061297	0.97661	0.14932	-0.12446	-0.50052
-0.18433	0.29301	0.57295	-0.435	0.26532	0.2676
0.20928	0.20756	-0.096083	-0.92958	-0.1803	0.24563
-0.56966	0.053807	0.16809	0.19797	0.29457	-0.0057674
-0.0010209	0.015449	0.30483	-0.35031	0.23934	0.17763
-0.47175	0.22685	-0.21546	0.2801	-0.076297	0.047214
0.16554	0.090785	-0.12729	-0.44912	-0.33654	0.15731
0.1304	0.25687	-0.08074	-0.38696	0.00050214	0.16701
0.089509	-0.41989	0.10878	-0.079077	-0.021866	-0.42677
-0.13054	-0.37519	0.41604	0.038118	-0.34326	0.33879
-0.83294	0.29958	0.26525	-0.10081	-0.39891	-0.35539
-0.080561	0.19136	-0.11631	-0.35512	-0.29829	0.073249
-0.061909	-0.28086	-0.053003	0.09401	0.0084871	0.23893
-0.031225	0.13821	-0.3552	-0.42362	0.11984	-0.12229
0.156 0.	-0.39944	15047	0.1323	0.021657	-0.30671
-0.059203	-0.10953	-0.43177	-0.20805	-0.22899	0.089842

Table4 shows The Validation of test Patterns without any training

DISCUSSION

With the above experiment has been shown that binary bits of text CAPTCHA can be stored in the network, it also indicates that the system is working properly for password validation and finding storing them using the model of Back Propagation of Artificial Neural Networks . Password strength is depending on the number of neurons in the model. According to performance curve the machine recognize the character of 10 epochs. Best validation performance is 21252. Table 4 shows the memorized input patterns of the network. Table 2 shows that the system is able to generate data based on pattern mapped earlier during the training and give excellent results for patterns never trained. TRAINLM function is used to train the network which gives best result as compare to all other function. It takes minimum time to train the network and minimum number of iteration to train the network.

Performance curve shows that machine recognize the character in first 10 epochs.

RESULTS

This paper proposed a technique of CAPTCHA storing and recalling based on Back Propagation model of Artificial Neural Networks.. According to result of training the performance curve CAPTCHA is recognised very easily without any pre-processing and segmentation. Back Propagation model is introduced to improve network performance, which can recognize the different character of the CAPTCHA image with minimum number of iterations.

REFERENCES

1. Tomoka Azakami, Chihiro Shibata, Ryuya Uda, "Challenge of Deep Learning against CAPTCHA with Amodal Completion and After-effects by Colors" 2016, 2157-0426.

2. Shailaja Tingre, Debajyoti Mukhopadhyay, "An Approach for Segmentation of Characters in CAPTCHA", ICCCA 2015,978-1-4799-8890.
3. Yu Hu[1,2], Li Chen[1,2*], Jun Cheng[3] , " A CAPTCHA recognition technology based on deep learning" IEEE 2018,978-1-5386.
4. Xiao Ling-Zi, ZHANG Yi-Chun , " A Case Study of Text –Based CAPTCHA Attacks" ,IEEE 2012, 978-0-7695.
5. Mengyuan Wang[1], Yuliang Yang[1], Mengyu Zhu[2], Jiaming Liu[3], "CAPTCHA Identification Based on Convolution Neural Network", IMCES 2018, 978-1-5386-1803.
6. Brian Cheung, "Convolutional Neural Networks Applied to Human Face Classification" International Conference on Machine Learning and Application, 2012, 978-0-7695 .
7. Yanping Lv[1,2], Feipeng Cai[1,2], Dazhen Lin[1,2*], Donglin Cao [1,2*], "Chinese Character CAPTCHA Recognition Based on Convolution Neural Network",IEEE 2016, 978-1-5090-0623.
8. Ye Wang, Yuanjiang Huang, Wu Zheng, Zhi Zhou, Debin Liu, Mi Lu "Combining convolutional neural network and self-adaptive algorithm to defeat synthetic multi-digit text-based CAPTCHA" IEEE 2017, 978-1-5090-5320.
9. Mengyun Tang, Haichang Gao, Yang Zhang , Yi Liu, Ping Zhang, Ping Wang " Research on Deep Learning Techniques in Breaking Text –Based CAPTCHAs and Designing Image –Based CAPTCHA", IEEE Transaction on Information Forensics and Security, October-2018 Vol. 13 , No.-10.
10. Rafaqat Hussain , Hui Gao, Raiz Ahmed Shaikh, Shazia Parveen Soomro, " Recognition Based Segmentation of Connected Characters in Text Based CAPTCHAs" IEEE International Conference on Communication Software and Networks, 2016, 978-1-5090-1781.
11. Tao Zhang[1], Honglei Zheng[2], Lele Zhang[3], " Verification CAPTCHA Based on Deep Learning", Proceeding of the 37th Chinese Control Conference ",July 25-27, 2018.