**PICTURE PASSWORD VALIDATION**

Submitted in partial fulfillment of the requirements for the award of degree

**Of**

**BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE**

**AND ENGINEERING**

**Submitted by**

**B Thanmai (N170572),**

**K Sathvika (N171254),**

**M Pratyusha (N171211),**

**G Shri Vardhan (N170928),**

**MD Iqbal (N170973).**

Under the esteemed guidance

**Of**

**Mrs. Bhavani (Assistant Professor)**

****

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES** **NUZVID, ELURU(DIST-521202)**

**RAJIV GANDHI UNIVERSITY OF KNOWLEDGE AND TECHNOLOGIES NUZVID,ELURU(521202),**

**ANDHRA PRADESH**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**DECLARATION CERTIFICATE**

This is to certify that the project entitled, “PICTURE PASSWORD VALIDATION” is submitted by B Thanmai (N170572),K Sathvika (N171254) ,M Prathyusha (N171211),G Shri Vardhan (N170928),MD Iqbal (N170973) to the department of Computer Science and Engineering, Rajiv Gandhi University Of Knowledge Technologies,Nuzvid for the submission of mini project report in III year B.Tech in Computer Science and Engineering is a bonafide work carried out under supervision and guidance during the academic year 2022.

**- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -**   **- - - - - - - - - - - - - - - - - - - - - - - - - -**

| **MR. S. Chiranjeevi** **Mrs.S.Bhavani** |
| --- |
| Assistant Professor Assistant Professor |
| **Head of the Department**  **Project Supervisor** |
| Dept. of CSE Dept. of CSE |
| RGUKT, Nuzvid RGUKT, Nuzvid |
|  |

**RAJIV GANDHI UNIVERSITY OF KNOWLEDGE AND TECHNOLOGIES NUZVID,ELURU(521202),**

**ANDHRA PRADESH**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**DISSERTATION APPROVAL CERTIFICATE**

This is to certify that the project entitled, “PICTURE PASSWORD VALIDATION” is submitted by B Thanmai (N170572),K Sathvika (N171254) ,M Prathyusha (N171211),G Shri Vardhan (N170928),MD Iqbal (N170973) to the department of Computer Science and Engineering, Rajiv Gandhi University Of Knowledge Technologies,Nuzvid for the award of Bachelor of Technology in Computer Science and Engineering, has been accepted by the external examiners and that these students have successfully defended the project viva in the Viva-Voce examination held today.

**- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -**   **- - - - - - - - - - - - - - - - - - - - - - - - -**

| **MR. S. Chiranjeevi** **Mrs.S.Bhavani** |
| --- |
| Assistant Professor Assistant Professor |
| **Head of the Department**  **Project Supervisor** |
| Dept. of CSE Dept. of CSE |
| RGUKT, Nuzvid RGUKT, Nuzvid |
|  |

|  |
| --- |

**RAJIV GANDHI UNIVERSITY OF KNOWLEDGE AND TECHNOLOGIES NUZVID,ELURU(521202),**

**ANDHRA PRADESH**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**ACKNOWLEDGMENT**

We would like to acknowledge and express our gratitude to the following people for their magnificent support in sharing their wisdom and knowledge to our successful completion of the final year project.

We would like to express our profound gratitude and deep regards to our guide **Mrs.S.Bhavani, Assistant professor**, Dept. Of Computer science and Engineering for her exemplary guidance, monitoring and constant encouragement throughout the B.Tech course. We shall always cherish the time spent with her during the course of this work due to the valuable knowledge gained in the field of reliability engineering.

We express gratitude to **MR.S.Chiranjeevi, Head of the Department**(CSE) and other faculty members for being a source of inspiration and constant encouragement which helped us in completing the project successfully.

We are thankful to the director, **Prof. G.V.R SRINIVASARAO** for giving this opportunity to do this project.

Our sincere thanks to all the batch mates of 2017 CSE ,who have made our stay at RGUKT-NUZVID, a memorable one.

Finally,yet importantly, we would like to express our heartfelt thanks to our beloved God and parents for their blessings, our friends for their help and wishes for the successful completion of this project.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**Table Of Contents**

**Chapter-1**

1.1 Introduction……………………………………………………

**Chapter-2**

2.1 Related work …………………………………………………..

**Chapter -3**

3.1 Proposed method……………………

**Chapter -4**

4.1 Implementation ………………………………

**Chapter - 5**

5.1 Results……………………………………………………..

**Chapter -6**

6.1 Discussions…….

**Chapter - 7**

7.1 Conclusion

**Chapter - 8**

8.1 Future Enhancement

**Chapter - 9**

9.1 Bibliography

| **Chapter-1** |
| --- |
| **INTRODUCTION** |

In this technical world, setting an apt password which is unique and secure is a complex task. Though many password suggestions are in use, there is a possibility of losing confidentiality as the same password is entered every time, there exists a chance of being caught by sniffers . To overcome this problem, a new password pattern is introduced in this project which involves selection of an image instead of entering password manually which in turn enhances confidentiality.

Humans are visual creatures that process and remember visual cues better than most other forms of data, and graphical passwords exploit just that.

The user can quickly remember graphical passwords, therefore there is no need to write down any passwords anywhere. Additionally, a graphical password is exceedingly tough to guess. Another form of identification method that is highly distinctive for an authentication system is face recognition. Greg Blonder first presented a graphical password system based on recollection in 1996. With this technique, the user creates a password by clicking on several spots on a photograph.

| **Chapter-2** |
| --- |
| **RELATED WORK** |

1.AlphaNumeric Password/PIN :These passwords contain an amalgamation of Letters,Numbers and Special Characters. In general the length of the passwords lies somewhere in between 8-14 characters. These can be cracked with a brute force attack by using a subset of all passwords therefore are very less secure.

2.Facial recognition : Facial recognition passwords are a way of authenticating the identity of an individual using their face. As it is still in their relative infancy stage these passwords are pretty vulnerable to surveillance and breach of privacy.

### 3.Draw-a-Secret /Pattern : Patterns are the most used and least secured form of authentication as it can be easily replicated by marks of the fingerprints left by the user on the display screen. Also there are only sixty thousand possible patterns so it can be cracked comfortably.

### 4.Image Generated Text - CAPTCHA : Captcha is distorted letters with alphabets and numbers or just a mix of capital and small letters and math based problems .The main downside of this authentication is that it is so effortless and is readable.

| **Chapter-3** |
| --- |
| **PROPOSED WORK** |

The main aim of our project is to give an image as a password. Inorder for the system to process your password it has to differentiate your image from a set of images in its database and display the label of the given image.

At the time of registration the user gives an image of his choice of any category and the user need to remember the category he has registered with.Using the category every time the user logs into the page he/she will be given a choice of selecting the category of password that he/she has taken at the time of registration.

The objective here is to let the system react and predict the category of the image with respect to the given input image . For this we will work with various machine learning algorithms. We will here try a few classifiers which let the system know and predict what exactly the user is asking for .Our work in this is to design a model that verifies the category of given image that belongs to.

| **Chapter-4** |
| --- |
| **IMPLEMENTATION** |

In this we have given a large set of images database of different categories that includes mountains,streets,glaciers,forests,seas and buildings as an input .The given subset of images are selected and uploaded to a google drive and from there we mount them into the colab notebook.

The loaded data sets are divided into training and testing data sets . The train dataset is given as an input to the classifiers which in turn creates and returns the model . The model will now be provided with a test data set in order to make the predictions according to the patterns observed during the training process.

The role of classifiers plays a key role in making the models which make the predictions more precise. Among well known classifiers we have tried using a few of them namely Random Forest,Gaussian Naive Bayesian,Gradient boost,Extra trees and Light GBM. These provided very disappointing results as the accuracy is less than 50% .

So , We have tried using an application of Convolution Neural Network (CNN) i.e. Inception

**Chapter 5**

**RESULTS**

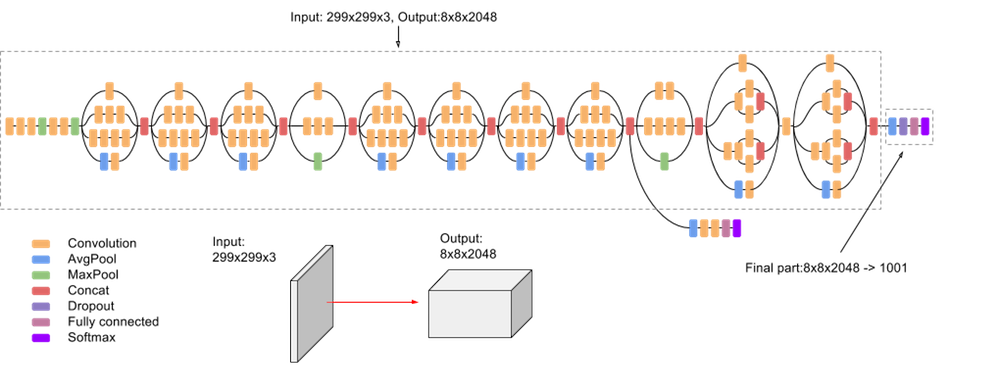
| **S.no** | **Classifier** | **Running time (in ms)** | **Guessing time(in ms)** | **Password strength** | **Error rate** | **Accuracy(%)** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Gradient Boost Classifier | 2440 | 32 | 40 | 60 | 41 |
| 2 | Extra trees Classifier | 157235 | 125 | 60 | 40 | 56 |
| 3 | Random Forest Classifier | 253463 | 70 | 60 | 40 | 53 |
| 4 | Gaussian Naive Basian | 2440 | 32 | 40 | 60 | 47 |
| 5 | Inception v3 | 354672 | 170 | 80 | 20 | 89.6 |

**Chapter 6**

**DISCUSSIONS**

Inception v3 is an image recognition model that has been shown to attain greater than 78.1% accuracy on the ImageNet dataset. The model is the culmination of many ideas developed by multiple researchers over the years. The model itself is made up of symmetric and asymmetric building blocks, including convolutions, average pooling, max pooling, concatenations, dropouts, and 48 fully connected layers. Batch normalization is used extensively throughout the model and applied to activation inputs. Loss is computed using Softmax.It can take an input of 1M data at a single run.

A high-level diagram of the model is shown in the following figure



**Our approach:**

According to the rules of architecture fixed weights are already assigned and no need to modify them.To get the best model and terminate it when the loss of ith an i-1th epoch we used callbacks and set the factor to 0.1

Callback:A callback is a set of functions to be applied at given stages of the training procedure. You can use callbacks to get a view on internal states and statistics of the model during training.some of the callbacks used are:

1.EarlyStopping:

min\_delta=1 means that the training process will be stopped if the absolute change of the monitored value is less than 1

2.ModelCheckpoint:

This callback saves the model after every epoch.

3.LearningRateScheduler:

It adjusts the learning rate over time using a schedule that you already write beforehand. This function returns the desired learning rate (output) based on the current epoch (epoch index as input).

We have used these callbacks in order to improve the accuracy of working of the algorithm .

| **Chapter-7** |
| --- |
| **CONCLUSION** |
|  |

As security and privacy are the most valuable assets to the users of this generation.A look at the advancement in technology over the past few years tells us that the next era will have system security at its core. So we have presented graphical passwords schemes that achieve better security than conventional textual passwords.

To address the problems with traditional authentications,we have focused on some other alternatives,using images as passwords.Graphical Passwords may be adapted in future as a major authentication system owing to its security. In this we are trying to make our authentication system more user friendly .For that we used Inceptionv3 to get more accurate results. So there should be extensive research on increasing the set of databases for security and better classifiers to attain cent percent accuracy.

| **Chapter-8** |
| --- |
| **FUTURE ENHANCEMENT** |

Graphical passwords are more user ready , secure and cost effective when compared to other secured based authentication methods like biometrics. So these may replace all traditional authentication methods in future . As biometrics are not affordable by everyone there is an utmost requirement to do extensive research in this field.

There are few drawbacks in this system regarding accuracy and shoulder surfing.

The main objective of any research or an innovation is to execute the required output with better accuracy within a given amount of time.

Even Though Inception played an important role in identifying the accurate password it takes an awful amount of time. So there is a real need for deep research in the inception classifier to minimize the running time for better productivity.

**Chapter 9**

**BIBLIOGRAPHY**

1.Pal, Bijeeta, et al. "Beyond credential stuffing: Password similarity models using neural networks." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.

2.Yang, Kunyu, et al. "VAEPass: A lightweight passwords guessing model based on variational auto-encoder." Computers & Security 114 (2022): 102587.

3.Lee, Kyungroul, et al. "Offensive Security of Keyboard Data Using Machine Learning for Password Authentication in IoT." IEEE Access 9 (2021): 10925-10939.

4.Singh, Vaishali, and S. K. Pandey. "Revisiting Cloud Security Attacks: Credential Attack." Rising Threats in Expert Applications and Solutions. Springer, Singapore, 2021. 339-350.

5.Xenofontos, Christos, et al. "Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies." IEEE Internet of Things Journal (2021).

6.Dong, Qiying, et al. "RLS-PSM: A Robust and Accurate Password Strength Meter Based on Reuse, Leet and Separation." IEEE Transactions on Information Forensics and Security 16 (2021): 4988-5002.

7.David, Liron, and Avishai Wool. "An explainable online password strength estimator." European Symposium on Research in Computer Security. Springer, Cham, 2021.

8.Zhang, Lei, et al. "Does the layout of the Android unlock pattern affect the security and usability of the password?." Journal of Information Security and Applications 62 (2021): 103011.

9. Belk, Marios, et al. "An Empirical Study of Picture Password Composition on Smartwatches." IFIP Conference on Human-Computer Interaction. Springer, Cham, 2021.

10.Guo, X., Liu, Y., Tan, K., Mao, W., Jin, M., & Lu, H. (2021). Dynamic Markov Model: Password Guessing Using Probability Adjustment Method. Applied Sciences, 11(10), 4607.

11. Vi, Bao Ngoc, Nguyen Ngoc Tran, and TrungGiap Vu The. "A GAN-based approach for password guessing." 2021 RIVF International Conference on Computing and Communication Technologies (RIVF). IEEE, 2021.

12.Wang, Jinwei, et al. "Modeling Password Guessability via Variational Auto-Encoder." 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE, 2021.

13. Emmadi, Nitesh, et al. "Privacy-Preserving Password Strength Meters with FHE." International Symposium on Cyber Security Cryptography and Machine Learning. Springer, Cham, 2021.

14. Dong, Qiying, et al. "RLS-PSM: A Robust and Accurate Password Strength Meter Based on Reuse, Leet and Separation." IEEE Transactions on Information Forensics and Security 16 (2021): 4988-5002.

15. Bai, Wenjie, Jeremiah Blocki, and Ben Harsha. "Password Strength Signaling: A Counter-Intuitive Defense Against Password Cracking." International Conference on Decision and Game Theory for Security. Springer, Cham, 2021.

16. Kanta, Aikaterini, et al. "How viable is password cracking in digital forensic investigation? Analyzing the guessability of over 3.9 billion real-world accounts." Forensic Science International: Digital Investigation 37 (2021): 301186.

17. Hartwig, Katrin, and Christian Reuter. "Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations." Behaviour& Information Technology (2021): 1-24.

18. Li, Wanda, and JianpingZeng. "Leet Usage and Its Effect on Password Security." IEEE Transactions on Information Forensics and Security 16 (2021): 2130-2143.

19. Zhang, Yi, Hequn Xian, and Aimin Yu. "CSNN: Password guessing method based on Chinese syllables and neural network." Peer-to-Peer Networking and Applications 13.6 (2020): 2237-2250.

20. Tolosana, Ruben, et al. "BioTouchPass2: Touchscreen password biometrics using time-aligned recurrent neural networks." IEEE Transactions on Information Forensics and Security 15 (2020): 2616-2628.