Freehand Sketch-Based Authenticated Security System using Convolutional Neural Network

S. Amarnadh, P. V. G. D. Prasad Reddy, N. V. E. S. Murthy

Abstract: ***An Authenticated Security System is a highly desired feature. In this paper, a FreeHand Sketch-based Authentication Security strategy is proposed for authentication purposes by allowing a user to choose one label from a collection of different labels and asking him to sketch the corresponding image for the selected label for registration to avoid mischievous registration and the sketched image gets preprocessed using adaptive threshold with Gaussian mixture and then predicted with a trained Convolutional Neural Network(CNN) data model to generate the necessary image label. The produced image label will compare with selected image label. If both are same then the details will store in the system database. The user gets login with his/her authorized details with sketch based image password. The image password gets preprocessed using adaptive threshold with Gaussian mixture and then predicted with a trained CNN model to produce the image name. The produced image name will compare with the system database for authentication. The methodology is tested with some sample input image passwords and the performance calculation is carried out using metrics like Recall and Precision. The proposed work exhibits the accuracy of approximately 85% by ensuring the authentication for the user security.***

Keywords: Security, Biometric systems, Authentication, Authorization, Security Patterns, Convolutional Neural Network(CNN), Free Hand Sketch Based Authenticated Security.

I. INTRODUCTION

Security is the major concern in the digital world, where data needs to be preserved and properly managed to the end-users. The security means to the digital data are provided to the end-user through authentication and privacy measures. The effective solution is providing the best authentication mechanisms to the end-users to keep their data secure. In recent years, with the development of several security patterns [1] there is a pool of well-proven generic solutions to the security problems [2]. The security patterns can be considered as a tool for non-security experts to provide a solution for security problems. In general, most of the web applications could provide the basic authentication pattern like username, passwordand in some cases, the re-authentication is possible with multiple actions.

The designers should mainly focus on providing security techniques to the end-users to protect their data.

The later techniques of ensuring security are Authenticator pattern [1] and Security Session pattern [2] where the Authenticator pattern concentrates on the subject's identity that needs to be verified basing on some information with the help of some protocol, before assigning proof of identity for the subject. In the context of securing patterns, the biometric systems [3] play a vital role in providing enhanced security for data protection. The general forms of biometric systems we possess are Fingerprint, palm, Iris scanners apart from the voice recognition system. The research is being carried out in the direction of computer vision strategies in more ways to provide much effective security mechanisms [4]. Therefore, the integration of images along with the conventions of username and password acts as an alternative way of securing the data of the users. The challenge or key issue in such forms of authentication is to provide vaguer space for the set of images to be maintained as a dataset provided by different users at the time of registration. Thus the designers or the researchers have to focus more on providing a more secure form of data privacy and user authentication process. The proposed research work focuses on providing multi-sketch pattern provision for the users to create at the time of registration so that along with user name and password the sketch provided by him is also acting as a mandatory option for authenticating the user thus provides more security for the information. The research work in the following sections includes methodology, architecture, and results derived from the proposed methodology called FreeHand Sketch-based [5] Authentication Security using CNN.

II. PROBLEM STATEMENT

Initially, the information systems were secured with text type passwords and then One Time Passwords(OTPs) were introduced for more security reasons. The Text type passwords can contain alphanumeric combinations such as numbers, alphabets and special symbols that are available in the computer keyboard. The authorized person could remember if the password is small, but at the same time, an unauthorized person could guess these passwords [6]. So, to secure the passwords from an unauthorized person there is a need to keep a large password making it unpredictable. In general, the text passwords are kept with the combination of relatives names, date of birth, cell number, therefore the unauthorized person can have the probability of guessing the passwords in different trials as shown in

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

S. Amarnadh, Assistant Professor, Department of CSE, GIT, GITAM (Deemed to be University), Visakhapatnam, India.E-mail: amarnadh07@gmail.com

Prof. P. V. G. D. Prasad Reddy, Professor, Department of CS & SE, A.U. College of Engineering, Andhra University, India. E-mail: prasadreddy.vizag@gmail.com

Prof. N. V. E. S. Murhty, Professor, Department of Mathematics, A.U. College of Science and Technology, Visakhapatnam, India. E-mail: drnvesmurthy@rediffmail.com

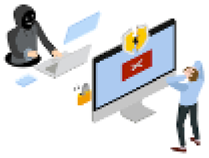


Fig. 1: Hacking Identity Theft System

Fig 1 by which the conclusion can be made stating that the text passwords are not safe [7]. As the next level of security, the combination of text passwords and OTPs are performed. Whenever the user gets login with his/her user Id and text password, then immediately he/she gets OTP to the registered mobile number. Unless and until he/she enters OTP is validated, the user is not allowed to perform the login. Even though it is secure, the OTP still has some key challenges like hacking by the unauthorized person using authorized mobile SIM using SIM SWAP techniques and social engineering [8]. In the current work, the advantage is the server consumes less memory to store the text type passwords and takes less processing time to verify the authorized details and to generate OTP to the registered mobile number, but the disadvantage is less security.

III. METHODOLOGY

In our proposed work, an extra security feature is appended to the information system that is, an image password that is trained using CNN. While comparing the text passwords with the image passwords, the images can be easily remembered [9] than the text. Till now two existing methods were considered for the login process namely Text Password and One Time Password(OTP). In this work, the proposal has been made by the appending of extra security features using a sketch type image password (Pattern) with CNN. In this method, the user is allowed to draw an image pattern with the help of a mouse in a desktop or with the help of a finger in a smartphone. If the image pattern is valid then the user can access his/her account otherwise the machine asks users to redraw the image password(pattern). The dataset has been considered from the QuickDraw dataset from Google with a group of 50,00,000 drawings with 344 different types.

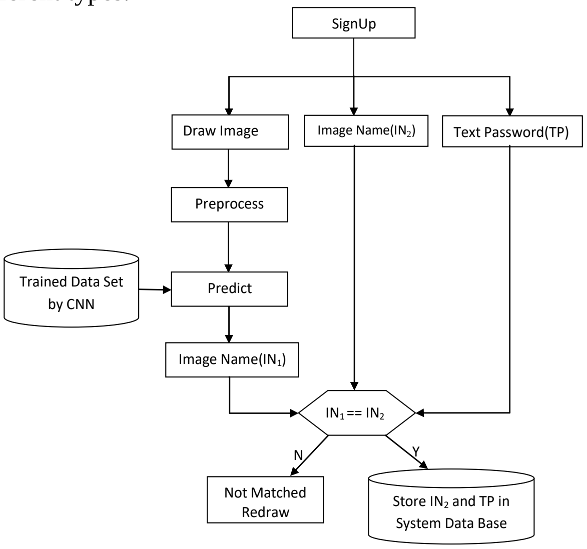


Fig. 2: Architecture of Image and Text Password Registration (SignUp)

A. Image Password Registration

The overall registration process of Image Password is illustrated in Fig.2 to register the image password and text password in the system database, the user needs to enter the details with text password and draw image password based on the selected image label from the given list. In the preprocessing stage, the adaptive threshold [10] is applied with Gaussian and inverse binary to give us better results for images with varying illumination. The obtained image is predicted with a trained CNN data model to generate the Image Name(IN1). Image Name(IN1) is compared with Image Name(IN2); if both are same then the user details, image name, and text password will store in the system database else request the user to redraw the image password.

B. Authentication/Validation:

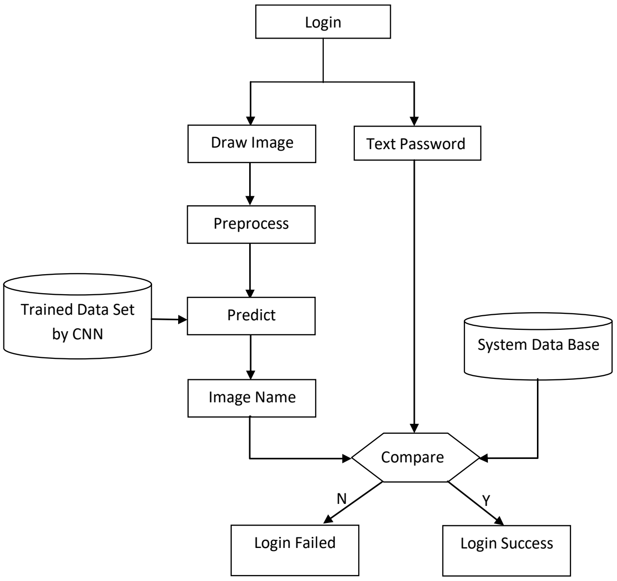


Fig. 3: Architecture of Image and Text Password Login

Overall login process of Image Password is illustrated in Fig.3, to authenticate the user is valid or not. The user enters details with a text password and will draw the image password. In the preprocessing stage, the adaptive threshold[10] is applied with Gaussian and inverse binary to give us better results for images with varying illumination. The obtained image is predicted with a trained CNN data model to generate the image name. Image name and text password will compare with the system database, if both are matching, then login pretends to be successful otherwise fails.

C. Adaptive Thres hold with Gaussian and Binary Inverse:

To generate a binary image, thresholding[11],[12], a grayscale image with a constant value is the method that is used regularly in image processing. For instance, in the grayscale image, any pixel value which is bigger than 100 can be fixed to 1 in the binary image, similarly, any pixel value which is equal or smaller than 100 can be fixed to 0. The above-specified method is known as fixed thresholding.

Retrieval Number: B4412129219/2019©BEIESP
DOI: 10.35940/ijeat.B4412.129219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

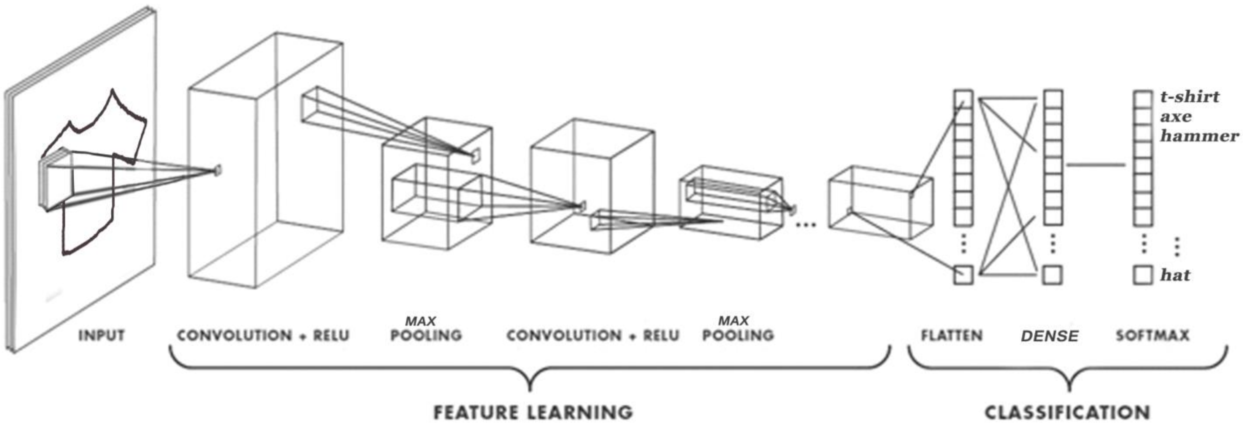


Fig.4. Convolutional Neural Network Architecture

In the adaptive threshold [10]basing on the adjacent(neighboring) pixel intensities the threshold values are calculated at each pixel position. In the image the threshold value TH(a,b) is computed at pixel position the below procedure needs to be executed:

Step I: m is chosen by the user, and m x m area around the pixel position is chosen.

Step II: The Gaussian weighted average[13],[14] of the pixel values which lie in the box are used to compute the weighted average of the mxm area and then more weight is given to the pixel values which are close to the center of the box. The value is represented by WTA(a,b).

Step III: To obtain the Threshold value TH(a, b) a constant parameter say, param1 is subtracted from the weighted average value WTA(a, b) computed for individual pixel in the last step. Therefore, threshold value TH(a,b) at pixel position(a,b) can be represented as

TH(a,b)=WTA(a,b)- param1.

- ***Threshold Binary Inverse***

Threshold Binary Inverse swaps the foreground and background colors in the processed image from 0 to 255 and 255 to 0 to achieve better results.

$$dst(a,b) = \begin{cases} 0 & if\ src(a,b) > TH(a,b) \\ mxVl & otherwise \end{cases}$$

Here a and b are pixel coordinates, mxVl is 255 and TH(a,b) is a threshold calculated per pixel. Therefore, in the proposed method, an adaptive threshold is applied with Gaussian and Inverse Binary to ensure better results for sketch-based images with varying illumination.

D. ConvolutionalNeural Network

The Convolutional Neural Network[5], [15], [16] is a research study under Deep Learning [17], with the class of deep neural networks, used for visual imagery analysis. It is the extended version multilayer perceptron which is a fully connected network where every respective neuron of layer 'n' is connected to whole neurons of another layer. As the multilayer perceptron form of full connectedness provides the flexibility of overfitting data, CNN can present the more complex patterns to assemble data using simple and small patterns following the shared weight architecture characteristics representing space invariant artificial neural networks(SIANN).

- ***Layers used in ConvNets:***

A simple ConvNet is constructed as a series of layers [18], where each layer converts the volume of activationsinto a different form using a differentiable function as shownin Fig 4. The construction of our ConvNet architecture includes fourlayers namely Convolutional, MaxPooling, Flatten, and Dense Layer.

- ***Convolution(Convol) Layer:***

ConVol Layer is the first layer of CNN where we can develop the data and image in general using filters. Now filters are small units that applied across the data through a sliding window. These filters are used to extract the features from an image as output and sent to the pooling layer as input. This ConVol layer is repeated three times in the proposed trained model with different types of filters.

- ***MaxPooling Layer:***

The MaxPooling layer is usually placed after the Convolution layer. The main aim of this layer is to decrease the spatial dimension of the input volume for the next layer. In this layer, the user applies some filters to select the max value from the selected region of the image which gives high-intensity pixel value to get the image more clarity. The effect of this layer is done on weight and height but not on the depth. In the proposed model MaxPooling layer had applied three times to decrease the spatial dimension of the input volume from 28x28 to 3x3.

- ***Flatten Layer:***

Flattening layer is the last stage of CNN which is used to classify the images for better results by converting the data into the 1-dimensional array to send it as input to its next layer. To generate a single long feature vector, the convolution layer output has been flattened. And it is connected to the fully-connected layer(dense layer) which is the last classification model. In the proposed model the output of MaxPooling layer 3x3x64 is flattened into 576 neurons.

- ***Dense Layer:***

It is also called as fully-connected layer. A linear operation in which each input is linked to each output with weight. So, there are m inputs and n outputs and therefore we have m x n weights. In the proposed model the dense layer is applied twice by implementing a dropout layer to overcome the overfitting problem by reducing neurons range from 576 to 128, 128 to 64.

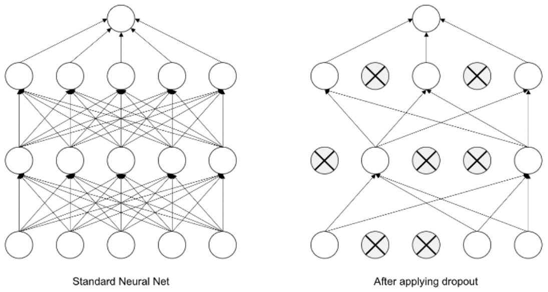


Fig. 5: Standard neural network model and the model after applying dropout technique

- ***Dropout Technique:***

Dropout is a regularization technique [19], [20] where randomly some neurons (both hidden and active) are ignored during the processof training the data set for decreasing the overfitting problem in neural networks as shown in Fig. 5. They are “dropped-out” randomly. When we have a huge amount of weight parameters and bias parameters then the artificial neural network tends to overfit the dataset problem for a particular use case.So, we have to find out the solution to solve this problem. There are two ways to solve the overfitting problem, a.Regularization and b. Dropout technique.

In the proposed model, the dropout technique is used to solve the overfitting problem. Initially select a dropout ratio to say like ‘p’, where ‘p’ is the range between 0 to 1 and choose a subset of features from the input layer, similarly select the subset of active neurons or inactive neurons from the hidden layer and this process repeats to the remaining hidden layers. Based on the input neurons we can assign p =0.5 using hyperparameter optimization for the first layer. Based on the p-value all the unselected neurons get removed from the hidden layers. By using this technique, the error rate get reduces.

E. ConvNets Trained Model:

The Convolutional Neural Network was trained with different layers [18] like Convolution, Max-Pooling, Flatten, and Dense Layer. In Fig. 6 it is shown clearly about the layers that we have applied in a step by step manner with different parameters as input to each layer. Initially, the first layer Convolution has taken the freehand sketch image as an input with size 28x28 then applied some 16 filters and forwarded it to the second layer Max_Pooling. The Max_Pooling layer reduced the image size from 28x28 to 14x14 and forwarded it to the third layer Convolution. This process was repeated for two more iterations by reducing the image size up to 3x3 and increasing the filters up to 64 and forwarded to the seventh layer Flatten. The Flatten layer transforms the input taken from the Max_Pooling layer into a single vector of 576 neurons. The dense layer is applied twice by implementing a dropout layer to overcome the overfitting problem by reducing neurons range from 576 to 128, 128 to 64. At last, the artificial neural network is implemented with some hidden layers and the output is generated.

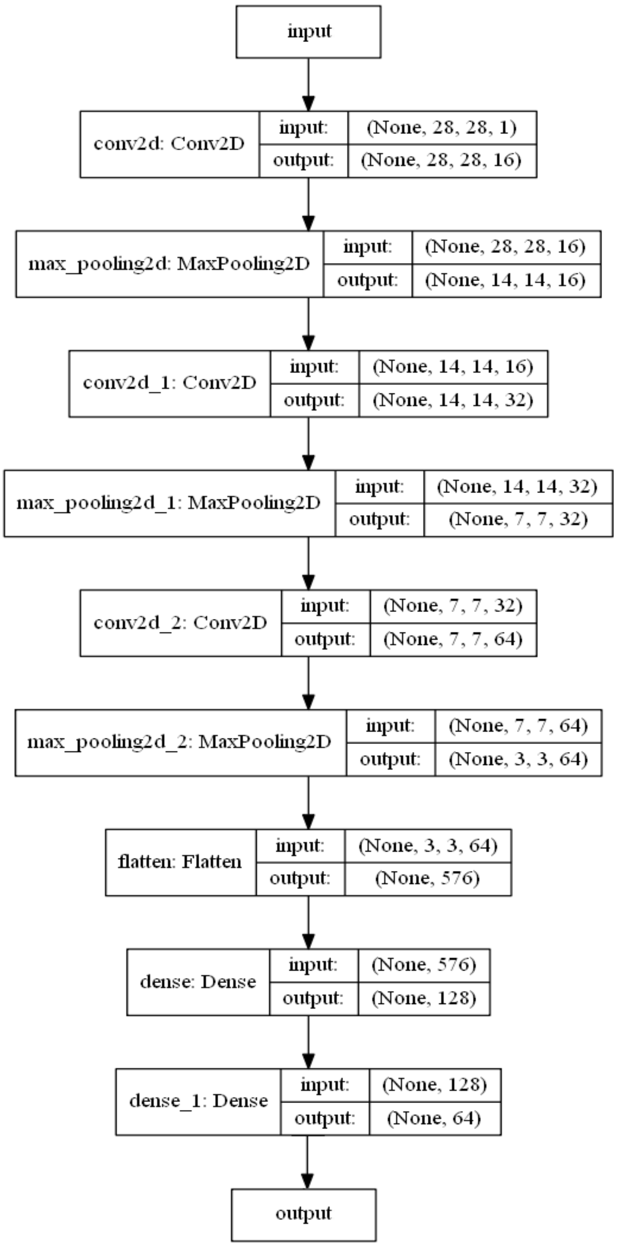


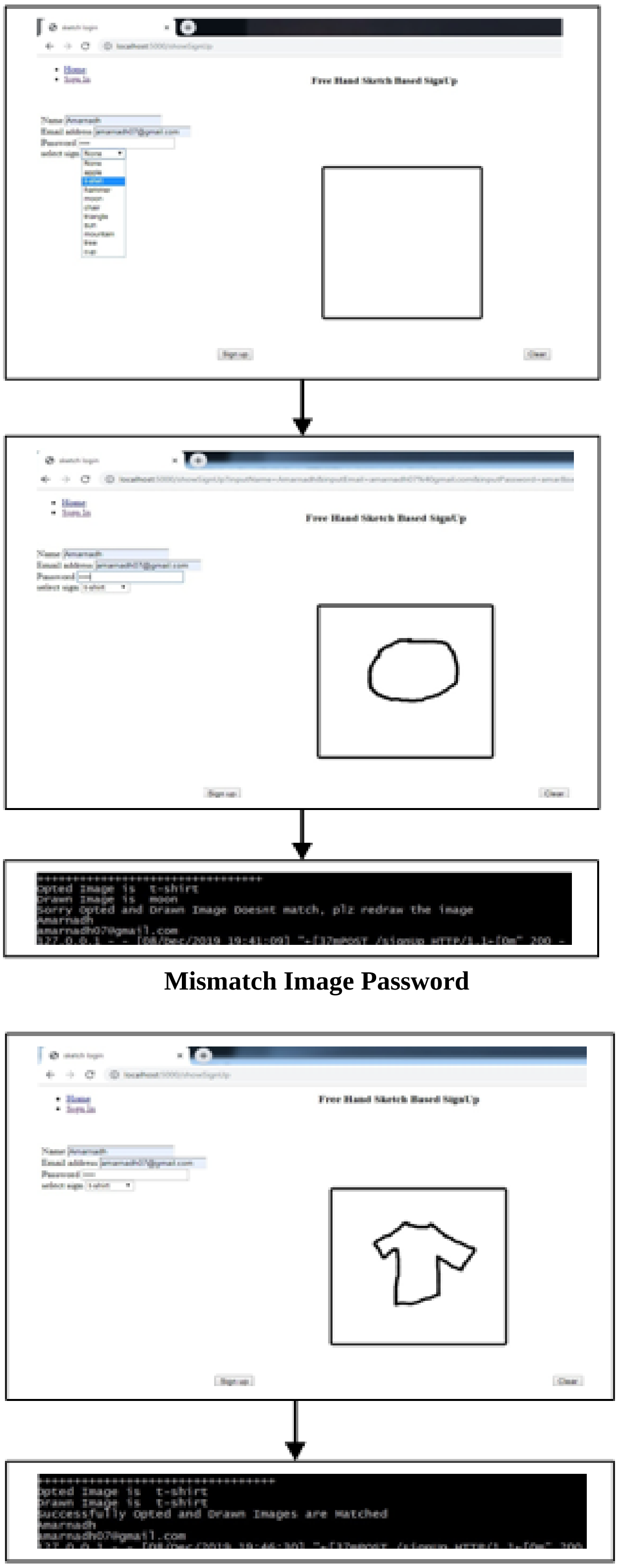
Fig. 6: Plot of Convolutional Neural Network Trained Model Graph

IV. EXPERIMENTAL RESULTS

In the proposed work, the experimentation is carried out on around 1000 sketches and 64 classes with 80%of different sketches were considered for training purposes and 20% for testing. The prototype system is implemented in python's latest version 3.6.5. and JSP. Initially, the user registers into the account by giving his/her details and selects the image label from the given list as shown in the below sample output screenshots and will draw the matching image pattern, otherwise, registration gets fail.

In the login process, the user enters the details with a text password and will draw an image password which is tested with the trained dataset by Convolutional Neural Network and generates the image name, then it is compared with the image label which is stored in the system database. The output screenshots are shown in figure7, 8.

Output Screen Shots of Image Password Registration:



Free Hand Sketch Based SignUp

- Home
- Sign In

Name Amarnadh
Email address amarnadh07@gmail.com
Password ••••
select sign None

Free Hand Sketch Based SignUp

Name Amarnadh
Email address amarnadh07@gmail.com
Password ••••
select sign t-shirt

```
++++++++++++++++++++++++++++++++++
Opted Image is  t-shirt
Drawn Image is  moon
Sorry Opted and Drawn Image Doesnt match, plz redraw the image
Amarnadh
amarnadh07@gmail.com
127.0.0.1 - - [08/Dec/2019 19:41:09] "←[37mPOST /signup HTTP/1.1←[0m" 200 -
```

Mismatch Image Password

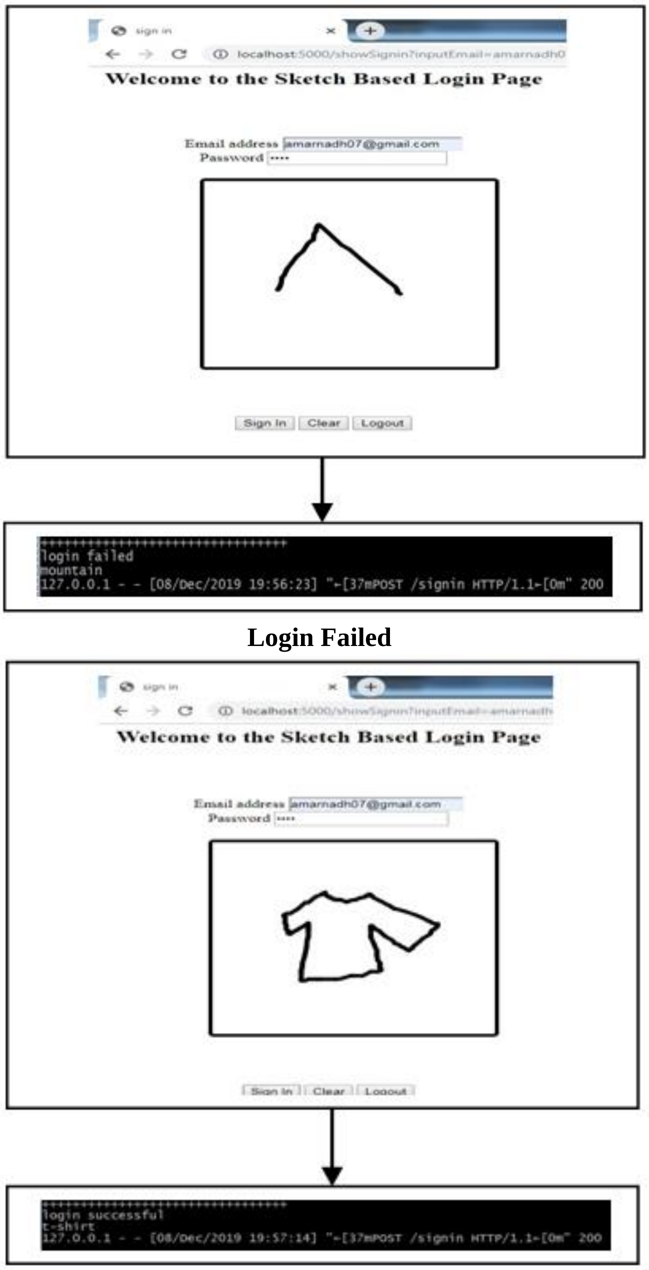
Free Hand Sketch Based SignUp

Name Amarnadh
Email address amarnadh07@gmail.com
Password ••••
select sign t-shirt

```
++++++++++++++++++++++++++++++++++
Opted Image is  t-shirt
Drawn Image is  t-shirt
Successfully Opted and Drawn Images are Matched
Amarnadh
amarnadh07@gmail.com
127.0.0.1 - - [08/Dec/2019 19:46:30] "←[37mPOST /signup HTTP/1.1←[0m" 200
```

Compatible Image Password
Fig. 7: Image Password Registration Process

Output Screen Shots of Authentication/Validation:



Welcome to the Sketch Based Login Page

Email address amarnadh07@gmail.com
Password ••••

sign in
localhost:5000/showSignin?inputEmail=amarnadh0
Sign In
Clear
Logout

```
++++++++++++++++++++++++++++++++++
login failed
mountain
127.0.0.1 - - [08/Dec/2019 19:56:23] "←[37mPOST /signin HTTP/1.1←[0m" 200
```

Login Failed

Welcome to the Sketch Based Login Page

Email address amarnadh07@gmail.com
Password ••••

sign in
localhost:5000/showSignin?inputEmail=amarnadh
Sign In
Clear
Logout

```
++++++++++++++++++++++++++++++++++
login successful
t-shirt
127.0.0.1 - - [08/Dec/2019 19:57:14] "←[37mPOST /signin HTTP/1.1←[0m" 200
```

Login Successful
Fig. 8: Login Process

A. Performance Evaluation

The performance of the model is compared using the results obtained from the models designed using Convolutional Neural Network. The comparison of results is made for evaluation of accuracy using the metrics namely, Precision and Recall [21]. The Precision, Recall and Accuracy are calculated based on the values of True Positive, True Negative, False Positive and False Negative. The accuracy result is best for balanced data. If the number of testing images is same in all the classes, then it is called as balanced data so, our proposed method Accuracy is calculated using the Metric Formula as shown in Table-I [22]. The results derived are tabulated and presented in Table-II.

Table I: Metric Formula of Precision, Recall and Accuracy

S.No.	Metric	Formula
1	Recall	$n(T_P)/(n(T_P)+ n(F_N))$
2	Precision	$n(T_P)/(n(T_P)+ n(F_P))$
3	Accuracy	$(n(T_P)+ n(T_N))/(n(T_P)+ n(T_N)+ n(F_P)+ n(F_N))$

Table II: Precision, Recall, Accuracy on CNN Image Password

Samples	Image Password	Out of 30 Trials				Precision %	Recall %	Accuracy %
		T_P	F_N	T_N	F_P			
1	t-shirt	25	5	29	1	96.15	83.33	90.00
2	tree	17	13	30	0	100.00	56.67	78.33
3	hammer	25	5	30	0	100.00	83.33	91.67
4	moon	23	7	20	10	69.70	76.67	71.67
5	chair	25	5	24	6	80.65	83.33	81.67
6	triangle	20	10	29	1	95.24	66.67	81.67
7	apple	19	11	30	0	100.00	63.33	81.67
8	sun	24	6	28	2	92.31	80.00	86.67
9	mountain	24	6	30	0	100.00	80.00	90.00
10	hat	28	2	29	1	96.55	93.33	95.00
Average						**93.06**	**76.67**	**84.83**

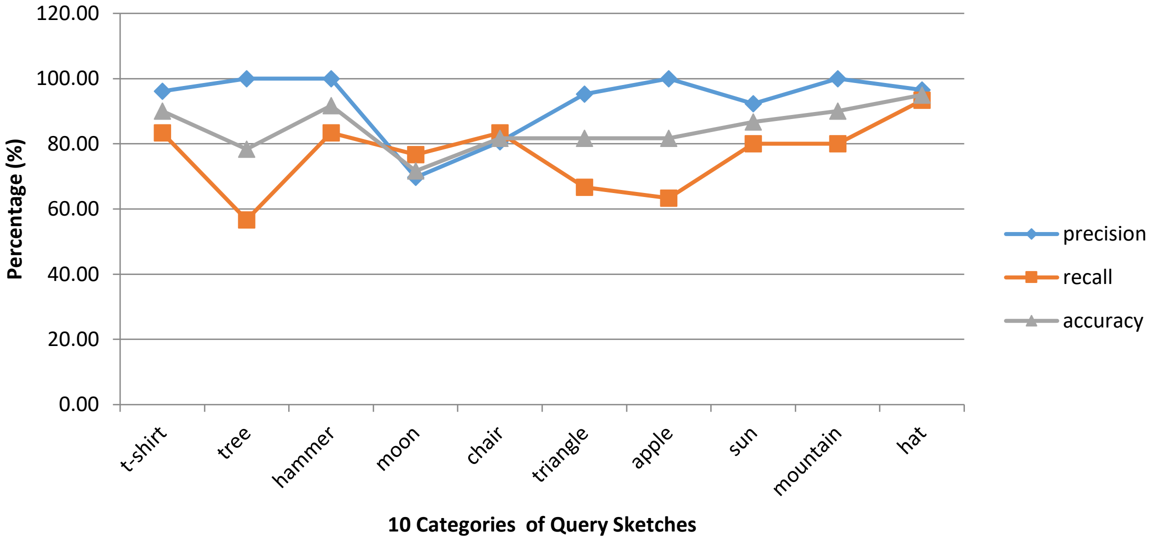


Fig.9: Precision, Recall and Accuracy of different sketchbasedpassword images

V. CONCLUSION

This paper presents a methodology for the FreeHand Sketch-based Authenticated Security System using Convolutional Neural Network. In general two methods of security are considered namely text-based and sketch-based password systems and tried to decrease the efforts required by end-user to remember passwords. The precision, recall and accuracy values for some sample password images are calculated using CNN individually. The results obtained are presented in Table-II. In the proposed methodology, the average precision, recall, and accuracy values were remarkable and the accuracy percentage of validating the authorized user is 84.83%. Precision, Recall, and Accuracy of 30 trails for 10 sample password images are shown in Fig. 9. The research in this direction can be improved better for recognizing an authorized user and also can secure our information system from hackers and this work may be personalized in the future as a major authentication system in the digital world.

REFERENCES

1. J. Yoder and J. Barcalow. 1998. “Architectural Patterns for Enabling Application Security”. In Pattern Languages of Programs Conference (PLoP).
2. E. B. Fernandez. 2013. “Security Patterns in Practice - Designing Secure Architectures Using Software Patterns”. John Wiley & Sons.
3. Mohamed Hammad ,Yashu Liu and Kuanquan Wang. “Multimodal Biometric Authentication Systems Using Convolutional Neural Network Based on Different Level Fusion of ECG and Fingerprint”, Volume 6, 2169-3536, 2018 IEEE.
4. SurabhiAnand, Priya Jain, Nitin and Ravi Rastogi. “Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication”, 2012 14th International Conference on Modeling and Simulation.
5. Wayne Lu, Elizabeth Tran. “Free-hand Sketch Recognition Classification”, CS 231N Project Report, 2017 - cs231n.stanford.edu.
6. Mohammed Awad, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. “Password Security: Password Behavior Analysis at a Small University”, ©2016 IEEE.
7. Aishwarya N. Sonar, Purva D. Suryavanshi, Pratiksha R. Navarkle, Prof. Vijay N. Kukre,“Survey on Graphical Password Authentication Techniques”, IRJET, Volume: 05 Issue: 02 | Feb-2018.
8. Anshul Kumar, Mansi Chaudhary and Nagresh Kumar, “Social Engineering Threats and Awareness: A Survey”, 2015, 2(11): 15-19.
9. Pauline Dewan. “Words Versus Pictures: Leveraging the Research on Visual Communication”, Partnership: The Canadian Journal of Library and Information Practice and Research, vol. 10, no. 1(2015).
10. PayelRoy, Saurab Dutta, NilanjanDey, Saurab Dutta, Sayan Chakraborty, NilanjanDey, Ruben Ray. “Adaptive Thresholding: A comparative study”, European Journal of Advances in Engineering and Technology, 2014 IEEE.
11. Pradnya A. Vikhar, P. P. Karde. “Content based Image Retrieval (CBIR) System usingThreshold based Color Layout Descriptor (CLD) andEdge Histogram Descriptor (EHD)”, IJCA,Volume 179 – No.41, May 2018.
12. Mehmet Sezgin, Bu¨lentSankur, “Survey over image thresholdingtechniquesand quantitative performance evaluation”, Journal of Electronic Imaging 13(1), 146–165 (January 2004).
13. Reynolds D, “Gaussian Mixture Models”. Li S.Z., Jain A.K. (eds),Encyclopedia of Biometrics. Springer, Boston, MA, 2015.
14. Ferhat Bozkurt, Mete Yağanoğlu, and FarukBaturalpGünay, “Effective Gaussian Blurring Process on GraphicsProcessing Unit with CUDA”, International Journal of Machine Learning and Computing, Vol. 5, No. 1, February 2015.
15. TuBuia, Leonardo Ribeirob, MoacirPontib, John Collomossea. “Sketching out the Details: Sketch-based Image Retrieval using Convolutional NeuralNetworks with Multi-stage Regression”, 2018 Elsevier B.V.
16. Zakhayu Rian, VinyChristanti, Janson Hendryli. “Content-Based Image Retrieval using ConvolutionalNeural Networks”, 2019 IEEE International Conference on Signals and Systems (ICSigSys).
17. Ashwini Patil1, Prof. Amit Zore. “Deep Learning based Computer Vision: A Review”, November 2018 | IJIRT | Volume 5 Issue 6 | ISSN: 2349-6002.
18. Ali FadhilYaseen. “A Survey on the Layers of Convolutional Neural Networks”, IJCSMC, Vol. 7, Issue. 12, December 2018, pg.191 – 196.
19. Jing Yang and Guanci Yang. “Modified Convolutional Neural NetworkBased on Dropout and the Stochastic GradientDescent Optimizer”, Algorithms 2018, 11, 28; doi:10.3390/a11030028.
20. Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, RuslanSalakhutdinov. “Dropout: A Simple Way to Prevent Neural Networks from Overfitting”, Journal of Machine Learning Research 15 (2014) 1929-1958.
21. Hossin, M.and Sulaiman, M.N. “A Review on Evaluation Metrics for Data Classification Evaluations”, International Journal of Data Mining & Knowledge Management Process (IJDKP) Vol.5, No.2, March 2015.
22. D Santhosh Reddy, R Bharath, P Rajalakshmi."A Novel Computer-Aided Diagnosis FrameworkUsing Deep Learning for Classification of FattyLiver Disease in Ultrasound Imaging", 2018IEEE 20th International Conference on e-HealthNetworking, Applications and Services(Healthcom), 2018.

AUTHORS PROFILE

Mr. S. Amarnadh is pursuing Ph.D in Andhra University and working as an Assistant Professor in the Department of Computer Science and Engineering, GITAM Institute of Technology, GITAM(Deemed to be University). His main research work focuses on Sketch-based Authenticated Security System.

Prof. P. V. G. D. Prasad Reddy is a senior professor of Computer Science and Systems Engineering and presently working with Andhra University college of Engineering, Visakhapatnam, India.

Prof. Nistala V. E. S. Murthy obtained his M.S. in Mathematics from University of Hyderabad, Hyderabad, Andhra Pradesh, M.S. in Software Systems from BITS, Pilani, M.S. in Mathematics from the University of Toledo, Toledo, OH-43606, U.S.A., and a Ph.D. in Mathematics from the University of Toledo, Toledo, OH-43606, U.S.A. He worked in various Uncertainty Theories and Their Applications in both Mathematicsand Computer Science.