Bio Touch Pass Coupled Authentication for Secured Access

Jananeev[1], Golda Dilip [2]

[1]SRM Institute Of Science And Technology,

Department of Computer science and Engineering,

SRM University,Vadapalani,Chennai,INDIA

jananeev025@gmail.com

[2]SRM Institute Of Science And Technology,

Department of Computer science and Engineering,

SRM University,Vadapalani,Chennai,INDIA

Abstract: OTP and password verification systems that require typing or graphics are vulnerable to security risks and information falsification. The Model suggests combining handwritten numbers with OTP-based authentication for secure data access. The Model provides better protection for accessing private papers and helps prevent data breaches and theft. When a keyboard input-based system is used for OTP or pin verification, the devices are susceptible to key logging attacks. In our model, the pin or OTP is validated using touch biometrics. On the mobile screen, users are given an interface to type the OTP/PIN numbers with their fingers or a pen. The handwritten numbers will be entered and compared to the produced OTP or pin. Handwritten numbers are specific to users and give an extra layer of security. An application for smartphones that uses a handwritten digit recognition model implements the model. Handwritten digits (0–9) collected from users and kept in the database will be used to train the model. To

ascertain if a pin is legitimate or not, each digit is compared to the information that has been stored. User identity-based authentication is provided via biometric information. Level 1 authentication is used in the initial phase to compare the user's fingerprint to the one they registered during the registration procedure. If the user's identity cannot be verified, they will not be allowed to access the handwritten OTP module.

Keywords: BiometricAuthentication, Convolutionalneuralnetwork, One-timepassword [OTP],Personal Identification Number [PIN],Two-factorauthentication.

1.INTRODUCTION

Mobilephonesplay a vital role in the present environment. Smart phones are used to fulfil most basic In the modern world, mobile phones are quite important. The most fundamental needs, such as communication, information, and financial transactions, are met by smartphones. With the ability to make payments through websites like Gpay and Paytm, which are connected to the user's bank accounts, smartphone usage has advanced. If the PIN/OTP number is compromised, users won't receive private data. More than a million people now use smartphones, and several billion people will someday use them. In banking, transactions with reliable data are crucial. Physical transactions are currently not as preferred as online transactions. Multiple virtual transactions are supported by banking, including opening a bank account via video chat, authenticating users before transferring money between accounts, making loan payments online, and opening deposit accounts online. All of these services decrease actual consumer bank visits, enhancing online transactions. Since banking services contain sensitive user information, it also safeguards user

information against dangerous software and hackers. Passwords like PIN (Personal Identification Number) and OTP (One Time Password) are used to give two-factor authentication in order to provide security to mobile banking users.

Customers of mobile banking are increasingly vulnerable to scams and imitation SMS communications. When customers' mobile phones are lost, sensitive or personal information on the device, such as a PIN number, an OTP, or a banking password, is also lost. In accordance with [1], numerous users created numerous passwords in January 2019 to access private papers including Gmail, bank accounts, and other personal information. The idea of two-factor authentication is not upheld when the PIN or OTP is revealed to unidentified individuals. Mobile malware, shoulder surfing, user behaviour, and the repositioning of intruders—commonly referred to as "Smudge Attacks"—are some of the mobile banking services' most pressing security issues. Smudge Attacks allow attackers to guess user-accessible lock patterns or passwords by imprinting their fingerprints on touchscreens of mobile devices. [2]. The two-factor authentication process entails two basic steps: I sending an SMS to the user's registered mobile number by the security service provider. ii) The user enters this PIN or OTP into the verification system. In some instances, this method also uses biometric data. With the addition of handwritten digit-based OTP/PIN validation, this paper model offers the conventional two-factor authentication system while also providing unique user identity. The Model is trained and tested on a database made up of numerous users' handwritten digits from 1 to 9. [11] The study paper demonstrates that general handwriting from people who were not present was included. The maximum-period signature is formed by joining the difficulties of this paper's minimum-period representation. The strategy backed here is Bidirectional RNN (BRNN). It is believed that the decoder is an autoregressive. Based on the strokes and particular style, it is demonstrated that this

text was handwritten. [12] This work exemplifies a way of action that includes a second authentication password as a stroke of each character or number time, screen brightness/contrast alteration, or a sensor-based authentication system. Equal Rates of Error (EERs) 4.0% The privacy of a user is invaded when an attacker gains access to that person's password. The display screen brightness, period, stroke, and sensor-based authentication programme are examples of password gestures that are thought to be features to recognise secret data. [13] Exploring touch data reveals two biometric characteristics, including user hand form and muscle behaviour. These characteristics are used to confirm the legitimacy of a password. Users' interactions with the device are significantly influenced by the screen size, the application, and the context of their physical activity, which can help to increase accuracy. [14] The average error rate of our refined technique is only about 3%, according to experimental data obtained solely by observing users' touch behaviour on an Android phone. In order to prevent the performance of a mobile phone from suffering, a user authentication mechanism should be of low computational complexity. In this work, Naive Bayes and Decision Tree were used. Correlation between the algorithm and the RBFN (Radial Basis Function Network Mechanism) and PSO (Particle Swarm Optimization) algorithms. [15] The study focuses on the training Epoch's network performance using 69 features produced through diagonal extraction. It should be noted that it requires 854 epochs to reduce the mean square error to a tolerable level. A diagonal feature extraction method is utilised to recognise handwritten characters that have been written off-line. [16] With an EER of 6%, this methodology extracts specific structural, distribution, and projection features from pre-processed images that are appropriate for depicting handwritten digit images. Deep neural networks incorporate a number of components for semantic recognition. [17] The human handwriting style methodology produces good results with a recognition rate of about 96% and is effective and accurate. 4% is the specified expected error rate. Characters were identified by a neural network

(NN) classifier utilising shape-based zoning features. The neural network used was called a pattern-net. [18] In this study, random forgeries with error rates between 3% and 8% are compared to skilled frauds with error rates between 21% and 22%. Doodles and patterns are hard for customers to recall because they are not used regularly. The Methodology employs the Sequential Forward Floating Search (SFFS) algorithm. [19] In order to obtain accuracy that is even greater than ensemble designs while reducing operational complexity and cost, a CNN architecture is designed in the study article. The accuracy of the feature map is 99.76 percent. The number pattern is recognised by this model. [20] The hybrid model, which combines both classifiers' core traits, achieves an identification accuracy of 99.28%. Convolutional neural networks (CNN) and support vector machines (SVM) are two techniques for deciphering extremely complex passwords.

Key Press, Pattern Drawing, and Fingerprint Authentication as Existing Methodology for User Identification and Promoting Signature Patterns Not Recognized Digitally to Authorize Customers are the Research Gaps discovered based on the Literature Survey.

2.Comparative study of algorithm

Algorithm credits an important role in research to prove the efficiency of data extraction and processing them.

Comparative study with respect to SVM-[Support Vector Machine],CNN-[convolutional Neural Networks] and MLP-[Multi-Layer Perceptron].

Table.1. Algorithm Comparison

MODEL	TRAINING RATE	TESTING RATE	EXECUTION TIME

SVM	99.98%	94.005%	1:35 min
MLP	99.92%	98.85%	2:32 min
CNN	99.53%	99.31%	44:02 min

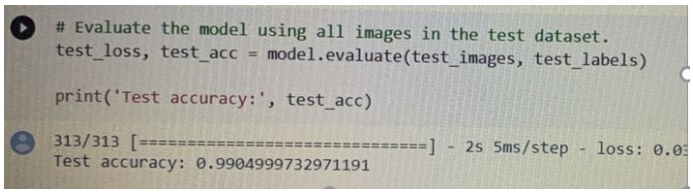


Fig.1. CNN Algorithm efficiency calculation for the Testing Dataset

The proportion of execution time for the Training and Testing data set is displayed in the comparative table1. In comparison to SVM and MLP, CNN executes more quickly. 99% of the time, CNN is accurate in identifying numbers. SVM demonstrated 94% accuracy in number recognition. MLP Accuracy displays a round-off accuracy of 98%. Without knowing anything about the training set, the CNN algorithm efficiently tunes the large data set. Unsupervised, semi-supervised, and supervised learning are all supported by the CNN algorithm. Based on the input received, the system learns and automatically extracts its feature. Multi-Layer Perceptron and image processing are driven by this algorithm. The data set won't be flattened by CNN at first. To increase its Efficiency and Data identification, the basic scenario is to crop the image and reduce the pixel size. Subsampling is the initial step, where the image is sampled to make it smaller. Convolution, the second stage in the algorithm, involves multiplying each pixel point to get the third Activation Function. In terms of parameter sharing and connection scarcity, CNN is effective. The weights of the filter are automatically determined by the CNN algorithm based on the input message.

In contrast, ANN users who wish to recognise photos must create a Filter Weight matrix. Its instinct is to assign a value to the image's outlines and a value of zero to empty regions. By multiplying the input vector by the filter weight, interpretation produces a feature map.

The equation is $Z = X * f^T$

where

X= input vector

f^T= filter weight

All filter weights are 3x3 matrixes. The input vector may be multiplied by any number of filter layers. Padding, which is the third stage, aids in returning the input image to its original size? The CNN algorithm includes an optional stream called padding. In the CNN algorithm's fourth stage, called Striding, the filter in the input image is traversed in one, two, or three steps. Including the final value for each stride in a matrix format. Pooling, which will determine the maximum value in each stride, is the fifth step in the algorithm. Pooling's purpose is to effectively reduce the geographic complexity of the computational network and use parameters.

2.1ARCHITECTURE DIAGRAM

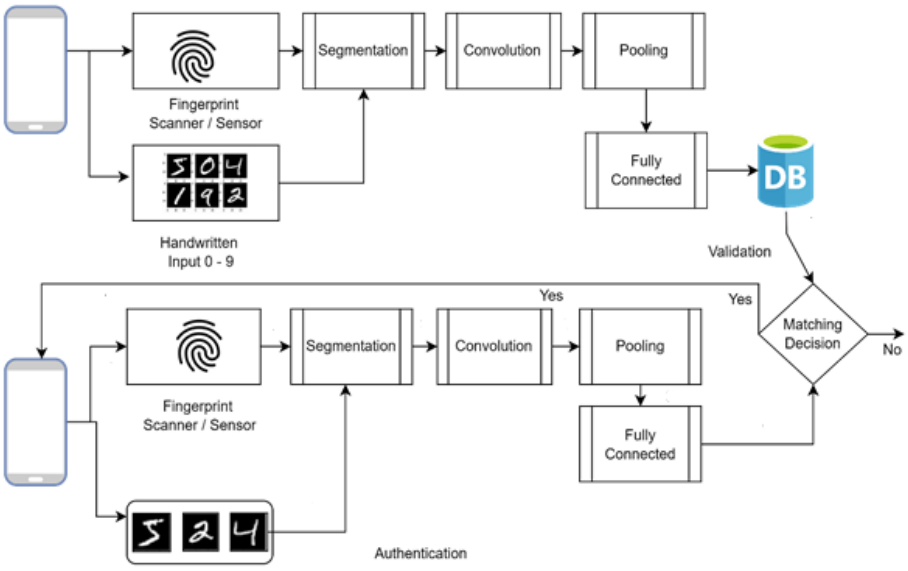


Fig.2. BioMetric Input based Authentication

Mobile phones capture the four digit OTP plus fingerprint sequentially for authentication .Each number is tagged with fingerprint to prove authentication .Gathered inputs are first segmented to remove noise and unwanted features .Using Convolution method the input vector is multiplied with random filters to identify the given data . Extracted output acts as a feature map which has maximum size to reduce its size we use Pooling .The Output which is pooled is mapped with output vector .There are two layers for one for training and other for testing phase. Testing phase have additional feature to make decision whether the given user is authorized person or not. Training phase ends up by updating new user finger print and new pattern of writing number in database .Testing phase ends up with authorization

3.Methodology

Theproposedmodelhastwophases.

i) Uniqueuseridentificationusingthebiometricimage ofthe user.

ii) Generating OTP and verifying if itmatcheswiththehandwrittendigits.

The suggested system offers an enhanced method for one-time password user authentication. Due to the fact that it offers authentication for seeing and updating confidential records, the system primarily targets users who needs high end security. The Model provides authentication based on the user's fingerprint information and handwritten digit recognition. This technology is provided as an improvement over conventional PIN-based systems, where the OTP is entered on a keyboard to secure user data. Using the registered fingerprint for authentication is the first step. A random OTP is generated if the user is legitimate. The user is given a canvas on which to write the numbers. The generated OTP is compared with the handwritten digit in order to identify it. The user gets authenticated if there is a match.

3.1 BIOMETRIC INPUT BASED AUTHENTICATION

The fingerprint is used for the initial step of authentication. At first, a new user must register their fingerprint. The manifest must contain the permission to Add Biometric before the fingerprint option can be added. Using the command below.

<uses-permission android: name=" android.permission.USE_BIOMETRIC"/>

When authenticating an app, it first determines whether fingerprint authorization is available and whether fingerprint authentication is turned on in the settings. Start a new activity

with the push of a button to establish a biometric dialogue. This starts a conversation on biometric authentication. theonAuthenticationError() and onAuthenticationSuccess() functions should then be implemented. If the app cannot recognise the fingerprint, it will fire onAuthenticationError(). If the fingerprint is found, the application will call onAuthenticationSucceeded().

3.2 DATA COLLECTION AND PREPROCESSING

The second module involves acquiring and preparing data. For this, this model makes use of the MNIST dataset. The dataset consists of 70,000 images of handwritten numbers from 0 to 9, which a CNN is being used to try to recognise. The Keras package includes the MNIST dataset, which makes it simple for us to load the dataset. 70,000 photos make up the dataset, of which 60,000 are used for practise and 10,000 for analysis. The images will be in AX train and AX test when the dataset loads, and the digits they represent will be in AY train and AY test once that process is complete. Each image in the MNIST collection has a size of 28 by 28 pixels. We must restructure our dataset. The inputs to the shape related to the training that the model needs are AX train and AX test. The majority of the pictures—60% for AX train and 10% for AX test—are of primary value. The user-inputted image is compressed with a framing size of 28 × 28 pixels. The representation of grey scale input is taken into account and always points to one. To better classify the supplied data, "One-Hot-Encode" divides the output class.

3.3 HANDWRITTEN DIGIT CLASSIFICATION USING CNN

The Convolutional Neural Network-based model that categorises the digits enables handwritten recognition. The input of manually typed numbers is converted into a matrix of 0–255 grey scale

values. The manually written integers are then saved as a bitmap and used to build a 28 × 28 matrix. After pre-processing, this is passed into the CNN-based Digit Classifier model.

The Model is constructed layer by layer and has a sequential nature. It contains two convolutional layers. Conv2D layers are used to process the two-dimensional images captured while the Matrix was in motion. Filter has 32 or 64 nodes for each of its two levels. Regarding bits positions, authentication sounds the kernel size. This kernel was created to map with a filter matrix and an input layer. The fit () function will be used by this model to create an output vector that combines input and hidden data. EPOCH () count, Target Data, and Training Validation are the fit () function's distracting features. Probability is shown in an array form based on the Training set [0-9]. The size of the kernel typically ranges between 3 x 3 and predicts the number with the highest likelihood of matching.

4.ALGORITHM

STEP 1: Dataset is collected

- Biometric input is obtained from the user as a registration step.
- Handwritten digit input is input that is used for testing and training the model.

STEP 2: Processing the data for use in the digit classifier model.

The handwritten digit input is in pixel values, ranging from 0 to 255, which is normalized.

STEP 3: Creating and training the CNN digit classifier model

Filters: The number nodes used is given by the filters, which is 32 and 64 for the two layers respectively. Kernel Size is 3 x 3 Matrix.

n: input f:Filter

Process 1: Building Blocks of a Convolutional Layer: **E**xtracting high-level input features from input data by passing those features to the hierarchy layer in the form of aspect maps.

Dimension Output Vector: (n-f+1)

$$y = f(x) = \Sigma x_i w_i$$

y (output) = sum (weights * inputs) + bias

y=output

xi= input vector upto i terms

wi=weights upto i terms

Process2:Pool Layer:

This layer reduces the dimensions of data by performing pooling on the feature map by generating maps with minimized dimensions.The maximum element from the region of the feature map covered by the filter is selected for pooling this process is known as maximum Pooling.

Example: Resultant matrix: 6 x 6,Strides: 3, Pooling :2 x 2 Matrix.

Process 3: Activation Function

Relu activation function is used to train, fit() function is used to correlate with the features of Training set, Epoch count and functional parameters with [target data,validation data].

Process 4: Fully Connected Layer:

Calculation ofprobability scores with respect to each label finally, the task of classification is

done by the FC layer. Matching with the trained set the ratio of highest probability is considered to be the best model fit.

```
model = keras.Sequential([
  keras.layers.InputLayer(input_shape=(28, 28)),
  keras.layers.Reshape(target_shape=(28, 28, 1)),
  keras.layers.Conv2D(filters=32, kernel_size=(3, 3), activation=tf.nn.relu),
  keras.layers.Conv2D(filters=64, kernel_size=(3, 3), activation=tf.nn.relu),
  keras.layers.MaxPooling2D(pool_size=(2, 2)),
  keras.layers.Dropout(0.25),
  keras.layers.Flatten(),
  keras.layers.Dense(10)
])
```

Fig.3. Simulation of CNN Algorithm

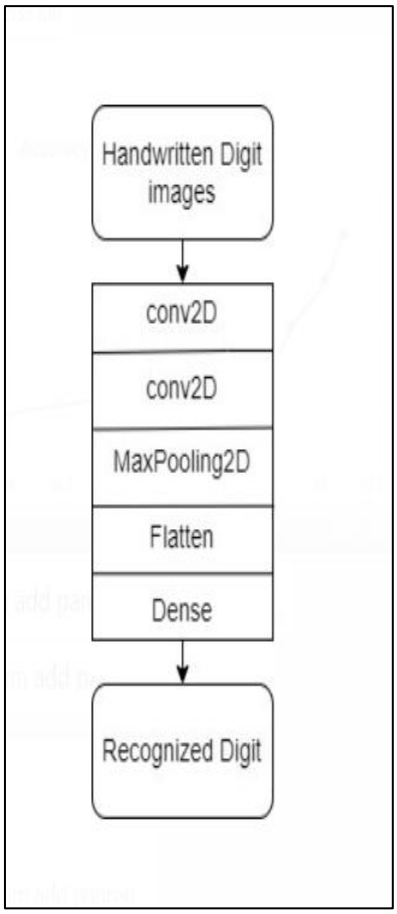


Fig.4. Flow of CNN Algorithm

4.1Working Model

Input Layer is considered to be 28 x 28 matrix the input image is multiplied with filter of size 3 x 3 matrix. The extracted output is applied with RELU Activation Function or Sigmoid Function.Extracted output is pooled using 2 x 2 Matrix which defines maximum Pool in each filter mapping using strides. Flattern() will identify the pixel for each output vector.

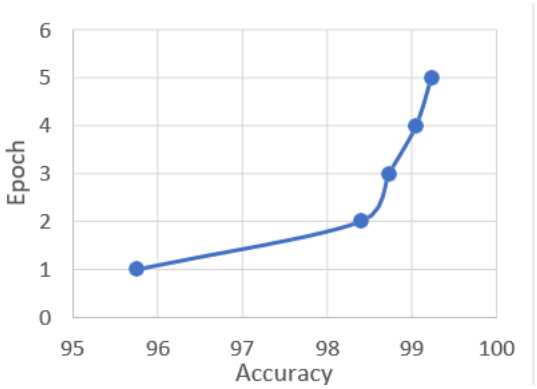


Fig.5. Accuracy of digit classifier model

4.2 Results and Discussions

4.2.1 Implementation of Fingerprint Authorization:

4.2.1.1 User Registration of Fingerprint:

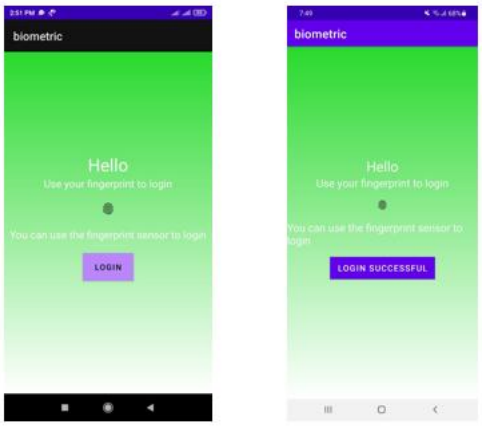


Fig.6. Finger Print Registration

User needs to key in his fingerprint for authentication.Trained fingerprints are stored in Bio-Database. [Bio-Database used to store human features as input].Once new user logs in the

system withfingerprint if the fingerprint matches user receives a message “Login Successful “or else Login Failed.

4.2.2Tagging Fingerprint and OTP each digit by drawing the pattern

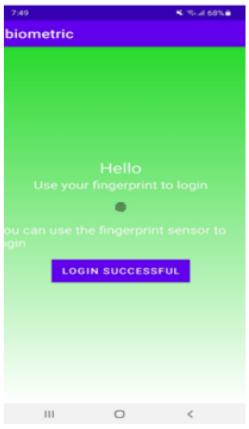
Bio Touch finger print Considered for Authentication	Machine Learning Trained Data set for numbers
	

Fig.7. Finger Print & OTP Verification

Training 0 to 9 digits using convolutional neural network which maps with the pattern in MNIST database as training set. Number that is drawn in the front of the app is matched with MNIST data image. It proves percentage ofcorrelation of the testing image with the trained image.Image can be drawn in any part of the screen which would be recognized with Trained set using CNN algorithm. This methodology will cut or crop the image where user has drawn the pattern.

4.2.3 MNIST CSV File with Trained 0 -9 digits:

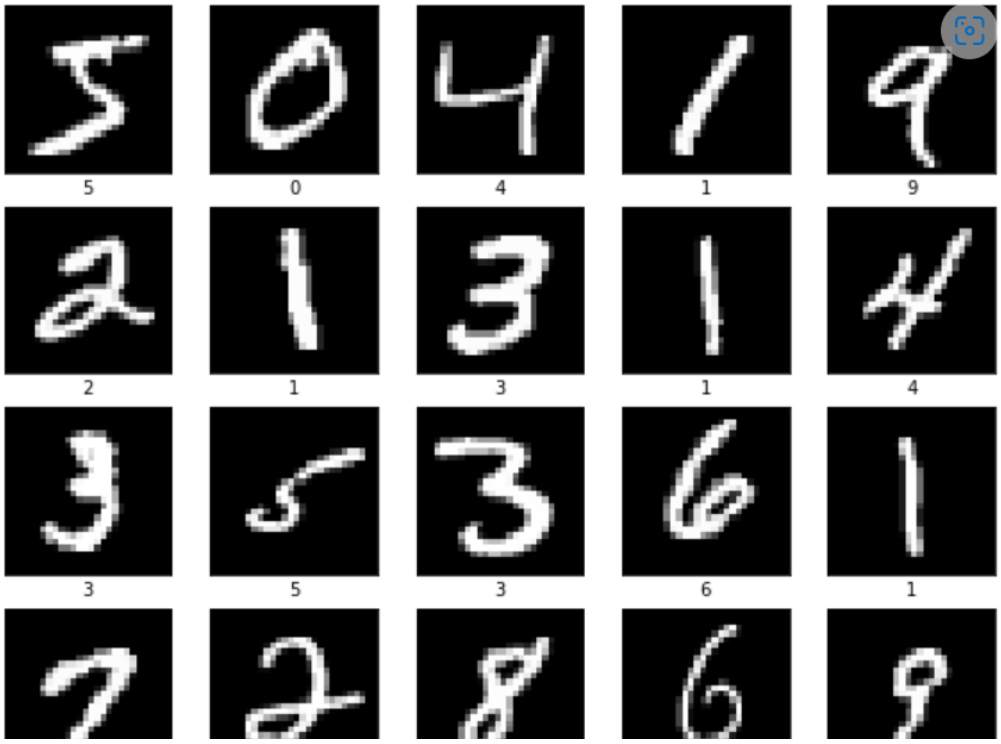


Fig.8. MNIST CSV File with Trained 0 -9 digits

data set containing numbers from 0 to 9 for training The many handwriting patterns are gathered and processed for optimum accuracy in number identification. In some ways, writing from different users is similar. Drawing patterns won't reveal the user authentication's uniqueness. Higher accuracy number identification is supported by this trained data set.

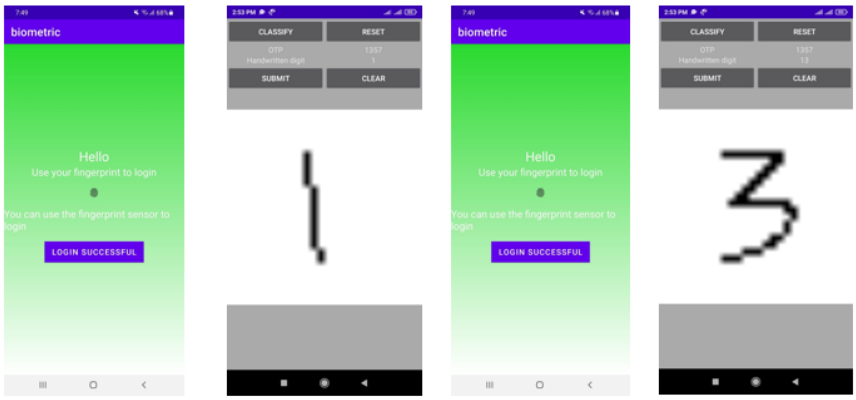
4.2.4 Implementation of Digit Recognition:

Fig.9. Digit Recognition Accuracy

Digit Recognition validates the accuracy percentage of each digit based on the testing results. The outcomes show that pattern drawing can successfully identify integers.

- Percentage of digit 5 Recognition :99.3%
- Percentage of digit 3 Recognition :98.7 %

4.2.5 Final Working of Digit Recognition:



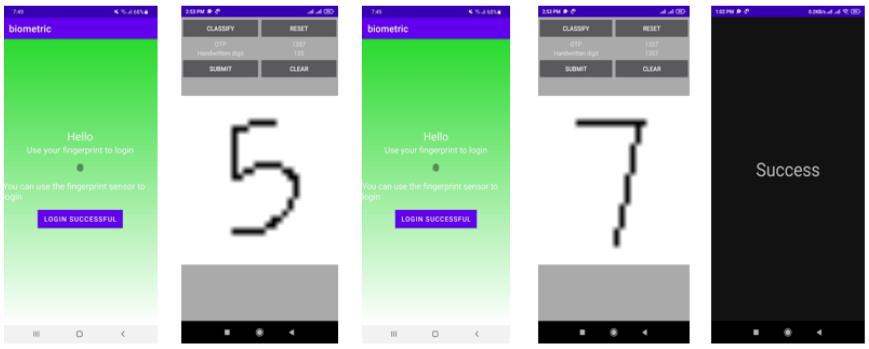


Fig.10. Working Model of Digit And Biometric

For a successful transaction, the OTP pattern will be authenticated with each digit. If the fingerprint and even one number don't match, the transaction fails. ensuring that the authorised user is accessible during the OTP. Knowing the OTP prevents unauthorised users from breaking in or accessing the system. The Model offers the highest level of security and protection for access to confidential documents.

5. Conclusion

In this study, handwritten digit-based OTP/PIN validation, which also enables unique user identity, replaces the conventional two-factor authentication method. Using a database of handwritten digits from 1 to 9 from various users, the model is trained and evaluated. As part of the two-factor authentication procedure, the security service provider sends an SMS to the user's registered cellphone number. This PIN or OTP is submitted into the verification system by the user. In some cases, this process also makes use of biometric data. The first step in our project is gathering data (digits) and verifying it. In the future, the data will be trained to recognise the user. more application and physical environments.

References

[1] RubenTolosana,RubenVera-Rodriguez,JulianFierrez,"BioTouchPass2:TouchscreenPasswordBiometricsUsingTime-AlignedRecurrentNeuralNetworks"inIEEETRANSACTIONSONINFORMATIONFORENSICSANDSECURITY,VOL.15,2020Article Cross Reference link.

[2] Marcos Faundez-Zanuy1,Julian Fierrez2; Miguel A. Ferrer3 , Moises Diaz4 , Ruben Tolosana2; "Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health"Springer : August 2020Article Cross Reference Link

[3] RubenTolosana,PaulaDelgado-Santos,Andres Perez-Uribe, Ruben Vera-Rodriguez,JulianFierrez,AythamiMorales,"DeepWriteSYN:On-LineHandwritingSynthesisviaDeepShort-TermRepresentations"in2021.Article Cross Reference Link

[4] VarshaM,NivethithaR,Mrs.SangeethaKrishnan, "Efficient Password Mechanism toOvercome Spyware Attacks" in InternationalJournalofResearchinEngineeringandScience(IJRES)ISSN(Online):2320-9364,ISSN(Print):2320-9356Article Cross Reference Link

[5] CaiyunMa,Hong Zhang "Discovery (FSKD) Effective Handwritten Digit Recognition Based on Multi-feature Extraction and Deep Analysis" 2020.Article Cross Reference Link

[6] Prof. Vaibhav. V. Mainkar, Mr. Ajinkya B. Upade, Ms. Jyoti A. Katkar, Ms. Poonam R,"Handwritten Character Recognition to obtain Editable Text" 2020.Article Cross Reference Link

[7] RubenTolosana,JavierGismero-Trujillo,RubenVera-Rodriguez,JulianFierrezandJavierOrtega-

Garcia,"MobileTouchDB:MobileTouchCharacterDatabaseintheWildand Biometric Benchmark"Article Cross Reference Link

[8] Anshul Gupta, ManishaSrivatsava ,ChitralekhaMahanta"Offline Handwritten Character Recognition Using Neural Network" 2011 IEEE Conference on ComputerApplications and Industrial Electronics (ICCAIE)Article Cross Reference Link

[9] RubenTolosana,RubenVera-Rodriguez,"BioTouchPass: Handwritten Passwords forTouchscreenBiometrics"inIEEETransactionsonMobileComputing,April2019 Article Cross Reference Link

[10] RubenTolosana,JavierGismero-Trujillo,RubenVera-Rodriguez,JulianFierrezandJavierOrtega-Garcia,"MobileTouchDB:MobileTouchCharacterDatabaseintheWildand Biometric Benchmark".Article Cross Reference Link

[11] RubenTolosna,RubenVera-Rodriguez,JulianFierrez,JavierOrtega-Garcia,"ExploringRecurrentNeuralNetworksforOn-Line Handwritten Signature Biometrics"inBiometricsandDataPatternAnalytics(BiDA) Lab-ATVS, Universidad AutonomadeMadrid,28049Madrid,Spain ,2018.Article Cross Reference Link

[12] Tao Feng, Xi Zhao, Nick DeSalvo,Tzu-HuaLiu,ZhiminGao,Xi Wang,,WeidongShi,"An Investigation on Touch Biometrics: Behavioural Factors on Screen Size, Physical Context and Application Context"2015Article Cross Reference Link

[13] YuxinMeng,DuncanS.Wong,RomanSchlegel,andLam-forKwok,"TouchGesturesBasedBiometricAuthenticationScheme for Touchscreen Mobile Phones" inConferencePaper·November2012Article Cross Reference Link

[14] Pradeep,E. Srinivasan, and S. Himavathi,"DIAGONAL BASED FEATURE EXTRACTION FOR HANDWRITTEN ALPHABETS RECOGNITION SYSTEM

USING NEURAL NETWORK"2015Article Cross Reference Link

[15] RubenTolosana,RubenVera-Rodriguez,JulianFierrezandJavierOrtega-Garcia,"Incorporating Touch Biometrics to MobileOne-TimePasswords:ExplorationofDigits"inConference,June2018Article Cross Reference Link

[16] Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally ,"Graphical Password-Based User Authentication With Free-Form Doodles",IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 46, NO. 4, AUGUST 2016Article Cross Reference Link

[17] SavitaAhlawat, AmitChoudhary, AnandNayyar, Saurabh Singh, Byungun Yoon "Improved Handwritten Digit Recognition Using Convolutional Neural Networks (CNN)" JUNE 2020Article Cross Reference Link

[18] SavitaAhlawata, AmitChoudhary," Hybrid CNN-SVM Classifier for Handwritten Digit Recognition"Procedia Computer Science volume 167 2020 Pages 2554 -2560.Article Cross Reference Link

[19] Zhun Li HyeYoung Lee Youngjun Lee SoojiYoonByeongilBaeHo-JinChoi,"HandwrittenOne-timePasswordAuthenticationSystemBasedonDeepLearning" in Journal of Internet ComputingandServices(JICS)2019.Feb.:20(1):25-37Article Cross Reference Link

[20] RubenTolosana,RubenVera-Rodriguez,JulianFierrezandJavierOrtega-Garcia,"Incorporating Touch Biometrics to MobileOne-TimePasswords:ExplorationofDigits"inConference,June2018. Article Cross Reference Link

[21] RubenTolosana,PaulaDelgado-Santos,Andres Perez-Uribe, Ruben Vera-Rodriguez,JulianFierrez,AythamiMorales,"DeepWriteSYN:On-

LineHandwritingSynthesisviaDeepShort-TermRepresentations"in2021.Article Cross Reference Link

[22] MarcosMartinez-Diaz,JulianFierrez,andJavier Galbally, "Graphical Password-BasedUserAuthenticationwithFree-FormDoodles"inIEEETRANSACTIONSONHUMAN-MACHINESYSTEMS,VOL.46,NO. 4,AUGUST2016Article Cross Reference Link

[23] Tao Feng, Xi Zhao, Nick DeSalvo, Tzu-HuaLiu,ZhiminGao,XiWangandWeidongShi,"InvestigationonTouchBiometrics:Behavioural Factors on Screen Size, PhysicalContext and Application Context" in 978-1-4799-1737-2/15/$31.00©2015IEEE2015Article Cross Reference Link

[24] Cheng-Lin Liu, Kazuki Nakashima, Hiroshi Sako, Hiromichi Fujisawa "Handwritten Digit Recognition Using State-of-the-Art Techniques"Proceedings Eighth International Workshop on Frontiers in Handwriting Recognition,2002.Article Cross Reference Link

[25] DejanGorgevik, DusanCakmakov "Combining SVM Classifiers for Handwritten Digit Recognition"Pattern 16th International Conference onVolume: 3,2002.Article Cross Reference Link

[26] EmanAlajrami, Belal A. M. Ashqar, Bassem S. Abu-Nasser, Ahmed J. Khalil, Musleh M. Musleh, Alaa M. Barhoom, Samy S. Abu-Nase "Handwritten Signature Verification using Deep Learning "2019.Article Cross Reference Link

[27] Ashwini Pansare, Shalini Bhatia "Handwritten Signature Verification using Neural Network "International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868, 2012.Article Cross Reference Link

[28] FathmaSiddique, ShadmanSakib, Md. Abu BakrSiddique"Recognition of Handwritten Digit using Convolutional Neural Network in Python with Tensorflow and Comparison of Performance for Various Hidden Layers".Article Cross Reference Link

[29] Abdullah Alshbtat, Mohammad Alfraheed, NabeelZanoon "A Novel Secure Fingerprint - based Authentication System for Student's Examination System"International Journal of Advanced Computer Science and Applications 10(9) 2019.Article Cross Reference Link

[30] Marfy, ArifulIslamNibras, ShamitIslam, Md.Naymul "FINGERPRINT-BASED BIOMETRIC AUTHENTICATION ACCESS CONTROL AND PERFORMANCE" 2021 Article Cross Reference Link