Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 6, 307-314 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Dense Deep Neural Network Architecture for Keystroke Dynamics Authentication in Mobile Phone

Lubna Abdelkareim Gabralla*

Department of Computer Science and Information Technology, Community College, Princess Nourah bint Abdulrahman University, 84428, Riyadh, Saudi Arabia

ARTICLE INFO

Article history:
Received: 18 July, 2020
Accepted: 29 October, 2020
Online: 10 November, 2020

Keywords:
Smartphones
Deep learning
Dense neural network

ABSTRACT

The ever-growing technology in mobile smartphones has enabled users to store sensitive and private information; as a result, it required the need for an improved security system. Previous approaches heavily relied on shallow machine learning algorithms that require feature extraction which is time consuming, laborious and can cause, resulting in poor authentication. In this paper, we propose a deep learning - dense neural network to avoid the limitation of the classical algorithms and build a mobile smartphone touch screen authentication scheme based on keystroke dynamics. A deep learning – dense neural network classifier was trained using keystroke dynamics features extracted from users. A comparative analysis was made between our proposed DNN classifier and some selected classical machine learning algorithms on the keystroke dynamics data. The data is split into five different data partition of training and testing. Results clearly indicated that the deep learning – dense neural network has eliminated the feature extraction steps required by the classical algorithms and improved the overall authentication accuracy, as such, improved the security of the smartphone device. In addition, it is found that the propose deep learning – dense neural network authentication scheme is more robust than the classical algorithms and has the potential to be fully implemented on smartphone to improve the security system of the mobile smartphone touch screen devices.

1. Introduction

The rapid advancement of technology in mobile smartphone devices makes them an important part of human life [1–4] . Also, the reduction in cost makes it easier for everyone to possess [5] including Those with disability,[6, 7] and their popularity is increasing [8, 9] They are now equipped with tremendous functionalities and a flexible operating system, providing the opportunity to store sensitive information such as official documents as well as installing official applications to improve the efficiency of office work [10]. Mobile phone users have become addict due to the social media applications and other applications being made available through google play store and apple store, [10] which carry numerous private information. Hence, the security of smartphone devices is becoming sacrosanct [11]. Protecting sensitive information requires a strong security scheme to protect the smartphone from intrusion, many mobile phone authentication schemes have proposed including person number (PIN),password and authentication [2] which are all vulnerable to shoulder surfing [2, 12]and smudge attacks [13, 14].Recently, biometrics have been incorporated into smartphone devices [15] in an effort to improve their security system . These include fingerprint auth entication and facial recognition. Fingerprint authentication is also vulnerable to attacks as a user's fingerprint can be copied from a touched object and used to gain access to the device [16]. Similarly, Facial recognition is also vulnerable to attack as the user's photo or video can be used to gain unauthorized access to the device and this attack is made easier as the pictures of users can be found on social media platforms [17].

The vulnerability to attack of the current security systems of mobile devices has led many researchers to propose different machine learning algorithms to improve their authentication scheme. For example, [18] they used support vector machine (SVM) to build a behavioral authentication scheme to improve the traditional authentication system. The scheme authenticates users

*Corresponding Author: Lubna Abdelkareim Gabralla, Email: lubnagabralla@gmail.com

https://dx.doi.org/10.25046/aj050637

Based on their behaviors when interacting with social media applications. It is found to perform better than other classical methods. As [19] presented a continuous behavioral authentication model to improve the security of mobile application. In the study, k-nearest neighbor (KNN), random forest (RF) and gradient boosting (GB) were used to build authentication classifiers. In [20], author built an authentication scheme using SVM based on physical activity performed by different mobile phone users. The proposed SVM model showed a promising result when compared with decision tree (DT) and KNN. In [21], the author hybridized SVM and hidden Markova model (HMM) to develop an authentication model using EEG signal while a user is drawing a pattern. The SVM-HMM model provides the best result when compared with naïve Bayes and cosine similarity. In [22], the author trained SVM classifier on facial attributes extracted from real images to build a continuous classification scheme. Results indicated that the proposed scheme shows a significant improvement on the existing continuous facial recognition system. Similarly, in [23] the author used a one-class SVM to build a behavioral biometrics authentication that automatically adapt to human behavior change over time while considering memory constraint. Results show that there is a possibility of using online machine learning to adapt to recent human behavior. In [24], the author trained a two-class SVM classifier using the user's SCG signal which captures heartbeat signal to improve the security scheme of smartphone devices. The heartbeat signal can be used as a unique feature to authenticate smartphone users.

In [25], the author explored four mobile phone non assisted sensors; transmitted data, noise, battery and ambient light to develop a continuous user authentication based on KNN. The KNN classifier achieved a reasonable accuracy. In [26], it exploits user's hand geometry and behavioral biometrics to build a one class classification model based on KNN. The model was compared with SVM and experimental results show that KNN outperforms the SVM in all the different positions. In [27] It creates an authentication scheme using artificial neural network (ANN) based on thumb stroke dynamics. The scheme was evaluated and compared with other .machine learning algorithms and the results of the experiment indicated that the ANN provided the best result. It was found that researchers in this domain heavily relied on SVM [28–33]; [18, 20–23] for mobile smartphone authentication. The previously used algorithms such as SVM, KNN, ANN etc. proved to be good in improving smartphone security especially when the data size is small. However, these algorithms require independent feature extraction before the extracted features are fed to the algorithms [19]. The performance of the algorithms depend on how well the features are extracted before modeling the classifier. Therefore, inefficient feature extraction may lead to poor classification accuracy [34] unlike deep learning which does not require independent feature extraction as it is done automatically and can work on large data size [35, 36]. Finally, a [37] convolutional neural network is applied to create an authentication scheme based on tap sequence and usage behavior of users.

In this paper, we proposed deep learning (dense neural network) based keystroke dynamics authentication for mobile smartphones touch screen device. The closest work to our proposal is [38] the one that employed deep learning technique to build an identification system that identify smartphone users based on keystroke behavior captured via a special keyboard or a web browser. This differs from our work in the sense that it focuses on a user's identification while our proposed model focuses on the user's authorization and authentication. Similarly, it explores gated recurrent unit and bidirectional recurrent neural network (GRU-BRNN) to build the identification model while our work explored the dense neural network. Also, [39] the deep neural network is explored to develop an authentication scheme based on user keystroke dynamics on mobile phone. Furthermore, our work explored supervise learning dense neural network on 71 different features of keystroke dynamics to build an authentication model while [39] applied deep neural network unsupervised learning on timing, tapping and inertial attributes of keystroke dynamics to develop an authentication scheme.

We choose the DNN in view of the fact that the learning features are provided from all the combination of the features in the layers while convolutional layer depends on minor repetitive field with features that are consistent [40].

The rest of the paper is structured as follows: Section 2 describes the concept of deep learning. Section 3 describes the methodology of the study. Section 4 presents the results and discussion before presenting Section five that comprises conclusions and recommendation for future work.

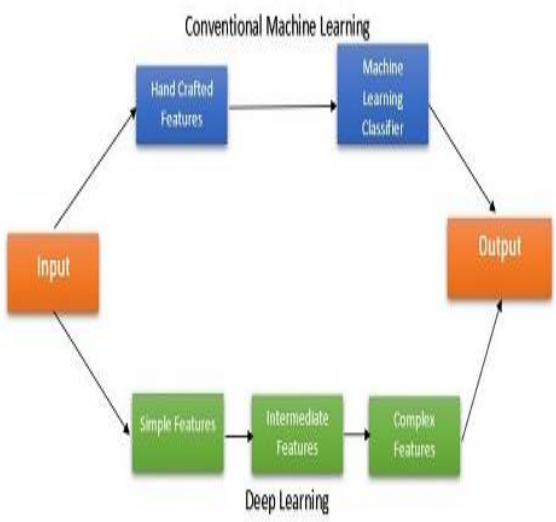

Figure 1: Conventional machine learning VS deep learning

2. Basic Concept of Deep Learning – Dense Neural Network

Deep Learning is an aspect of machine learning which represents multiple hidden layers that can learn on multiple attributes to produce better results [36]. Traditional machine learning algorithms have limitation on processing real data. Building a classification model with conventional machine learning algorithms, requiring reasonable amount of human expertise and efficient feature engineering to transform the raw data to desirable features that can be fed into any learning system or classifier. Deep learning permits inputting raw data into the algorithm without being transformed to feature vector or feature engineering as the features are learnt automatically during training the network [36].

Problems are solved in a hierarchical manner in deep learning, where the lower layers depict the basic representation of the problem and the upper layers are created based on the lower layers to build a more complex model. Deep learning is a hierarchical process as each layer in the deep learning network uses the output of the previous layer and the output of the current layer serves as the input to the successive layer to continuously build a complex concept [36]. The number of layers in a network determines the depth of the network. Cconventional machine learning only focuses on one or two layers, whereas in deep learning, the network contains at least three or more hidden layers. The unique aspect of deep learning is that the feature layers are automatically learned on the raw data not extracted by human expertise unlike the conventional machine learning[36]. The major advantages of deep learning over traditional machine learning are; automatic feature extraction and efficient handling of massive amount of data as a result, it keeps improving as the data gets larger [36]. Based on the concept presented in[36], we created Figure 1 to show deep learning and the conventional machine learning processes.

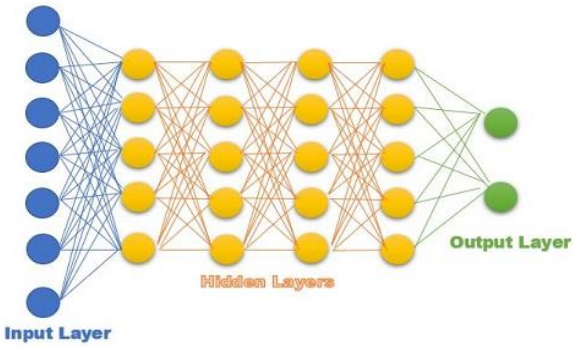

Figure 2: A simple example of dense neural network

In DNN, the layers of the network are fully connected as the name (dense) suggest, each neuron in a layer is connected to all the neurons in the previous layer which means all the nodes are fully connected to the nodes in the next layer. A densely connected layer learns features from all the combined features of the previous layer. The goal of the classifier is to adequately categorize the input data [40]. Figure 2 presents the simple example of DNN.

3. The proposed deep learning - dense neural network authentication model

This section presents the methodology of the study, where the data collection procedure, propose authentication model, propose work flow and performance metrics are outlined. The proposed model authenticates smartphone users is based on user's password typing behavior on a touch screen. The framework consists 4 steps namely; accusation of data, training, user authentication and performance evaluation.

3.1. Dataset

The dataset used for this study contains keystroke dynamics (user typing behavior) data of users collected from nexus 7 touch screen smartphone device when typing the "tie5Roanl" password. The data was collected from 56 subjects and each subject was asked to perform the task 51 times. Therefore, the dataset contains 2856 records. The dataset contains 71 attributes (features), the main features include: hold, up-down, pressure, finger area, average of hold, average pressure and average finger area. Each feature has some feature elements which correspond to the typed characters. The dataset is obtained from the UCI machine learning repository [41]. It was normalized between 0.00 – 1.00, consisting of the user's keystroke dynamics. The data extracted from touch screen smartphone is used to conduct the experiment. The dataset was partitioned several times and the keystroke attributes were used to train the deep learning – DNN classifier model. During the authentication phase, user's tested data for all the 56 subjects. As such, the classes are 56 to authenticate each of the 56 subjects. Each of the 56 subject is authenticated. If the similarities between the two models for each of the 56 users matches, the user is authenticated into the smartphone else the user is rejected. To evaluate the performance of the proposed deep learning model - DNN, the model is compared with previously used machines learning algorithms such as SVM, ANN and KNN. These three algorithms were chosen because the algorithms are found to be highly relied on especially SVM in creating classifiers for improving the security of mobile smartphones device [42].

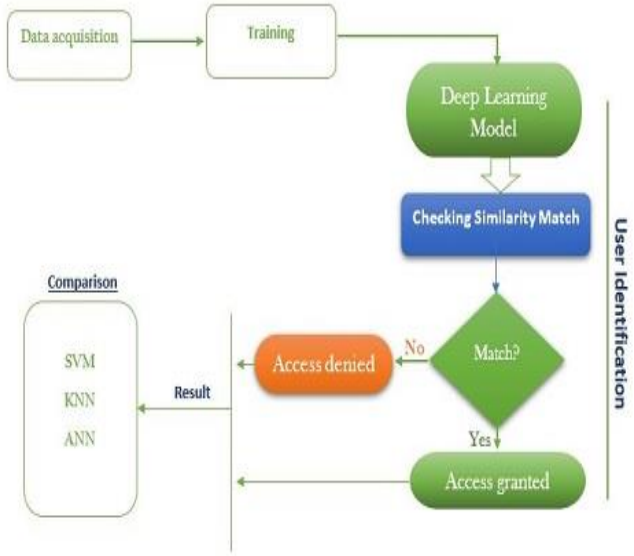

Figure 3: proposed model workflow

The SVM, KNN and ANN were trained to build classifier based on the keystroke dynamics data for the purpose of validation. The performance of the proposed deep learning - DNN classifier is compared with that of the SVM, KNN and ANN. The process involved assessing how well the algorithms perform on the test dataset. The performance of the algorithms on the keystroke dynamic dataset is measured based on performance evaluation metrics. The complete work flow of the methodology is presented in Figure 3.

3.2. Performance Evaluation Metrics

The performance of the proposed touch screen authentication model is evaluated using the true positive (these are instances that are correctly identified), true negative (instances that are correctly rejected), false positive (these are instances that are incorrectly identified) and false negative (these are instances that are incorrectly rejected). The performance metrics were computed

from the results generated from the validation of the models. The performance of the deep learning - DNN algorithm and the classical algorithms are being evaluated using the performance metrics [43].

Table 1: Summary of evaluation metrics

Evaluation metrics	Description
False Positive Rate (FPR) = $\frac{FP}{(FP+TN)}$	Used to determine how many instances are wrongly classified.
F1-Score = $\frac{2TP}{(2TP+FP+FN)}$	Determines the harmonic average between precision and recall.
Recall $(r) = \frac{TP}{(TP+FN)}$	Used to determine how many instances are been classified correctly.
Accuracy (A) = $\frac{TP+TN}{(TP+TN+FP+FN)}$	This is used to measure the accuracy of the technique.

4. Results and Discussion

In this section, the results generated from the experiment were presented including the discussion. The hardware platform, parameter settings of the proposed deep learning - DNN, comparative analysis of the DNN performance compared to the state of the art methods: SVM, ANN, and KNN were presented as well as the implication of the result in theory and practice.

4.1. Parameter Setting

The implementation was conducted on a platform equipped with Microsoft Window 10 with the following specifications:

- System Type: x64-based processor, 64-bit Operating System
- Memory installed on system (RAM): 8.00 GB
- Processor: Intel(R) Core (TM) i3-4000M @ 2.40 GHz 2.40 GHz

The platform for DNN is TensorFlow using Python. a preliminary experiment was conducted to obtain the best parameters of the propose deep learning - DNN. The number of hidden layers and the nodes on each hidden layer are selected after different combination of layers and nodes were run during the preliminary experiment. It was found that the deep learning - DNN setting with the best performance is presented in Table 2. Different learning rates were tested ranging from (0.1 - 0.9), the best value was adopted. Adam optimizer provided the best performance when compared with Gradient Descent Optimization and Adagrad Optimizer. Relu activation function was selected after been compared with other activation functions such as softmax, tanh, etc. The summary of the preliminary experiment result for setting the deep learning – DNN is presented in Table 2.

Table 2: Optimal parameter setting for the proposed DNN

Parameter	Setting
Input layer neuron(s)	71
Hidden layer 1 neuron(s)	20
Hidden layer 2 neuron(s)	20
Hidden layer 3 neuron(s)	20
Hidden layer 3 neuron(s)	20
Output layer neuron(s)	56
Learning rate	0.1
Optimizer	Adam optimizer
DNN structure	71-20-20-20-20-56
Epoch	1000
Activation Function	Relu Activation Function

The deep learning – DNN with the parameter setting in Table 2 is applied to run on keystroke dynamic datasets to authenticate access to mobile smartphone touch screen device. The DNN was run 10 times to ensure consistency of the result produced by the DNN. Data partition ratio affects the performance of the DNN, as such, several partition ratios were used to ascertain the robustness of the DNN and it is performance. An algorithm intend for real world application should be robust in addition to performance. The performance metrics in Table 1 were used to measure the performance of the DNN in user authentication for the mobile touch screen device. To evaluate the performance of the DNN, the classical algorithms SVM, KNN and ANN were also applied on the same dataset to authenticate user access to the touch screen mobile device based on keystroke dynamic authentication. The results of the experiments are presented in Tables 3 – 6 and Figure 4. The first column indicates the different data partition ratio used to evaluate the algorithms. The second column shows the algorithm for the experiment while the third, fourth and fifth columns indicate the mean, best and the worst performance respectively. The bold values in each Table indicates the best result obtained.

Table 3: Performance comparison of the propose DNN with the SVM, KNN and ANN based on Recall

Partition	Algorithms (%)	Mean (%)	Best (%)	Worst (%)
90-10	DNN	89.7	**96.0**	89.0
	SVM	68.7	73.7	51.7
	KNN	44.6	47.7	34.5
	ANN	2.57	3.5	1.8
80-20	DNN	91.2	**94.0**	86.0

	SVM	70.8	72.2	69.7
	KNN	44.6	46.1	43.7
	ANN	2.02	2.3	1.8
70-30	DNN	95.0	**99.0**	92.0
	SVM	71.3	72.7	70.1
	KNN	42.7	45.2	41.2
	ANN	2.1	2.3	1.8
60-40	DNN	93.1	**97.0**	89.0
	SVM	70.4	71.5	68.7
	KNN	41.7	42.4	41.1
	ANN	2.0	2.3	1.7
50-50	DNN	93.0	**98.0**	91.0
	SVM	68.8	69.3	68.2
	KNN	40.4	41.2	40.2
	ANN	1.9	2.2	1.7

The result presented in Table 3 represent the performance of the algorithms based on the Recall for the five different data partitions. It clearly shows that the proposed DNN model produce the best results compared to the classical algorithms. The DNN result indicates that the propose DNN classifier was able to authenticate user access to the mobile touch screen device based on keystroke dynamics with very high level of accuracy. Meaning that the DNN determines the number of instances that were correctly classified as the legitimate user of the mobile phone touch screen device. ANN produced the worst result in all the different data partitions. This is not surprising because the shallow ANN produce poor result as data size increases.

Table 4 clearly indicated that the propose DNN outperforms the classical algorithms in terms of the F1-measure. The performance of the DNN is far more than that of the classical algorithms recording more than 90% in each case. The ANN has maintained consistency in producing the worst performance in all the data partition ratio. This result means that the DNN is a good algorithm with potential to determine the harmonic average between the precision and the recall better than the classical algorithms.

Table 4: Performance comparison of DNN with SVM, KNN and ANN based on F1-Score

Partition	Algorithms (%)	Mean (%)	Best (%)	Worst (%)
90-10	DNN	89.6	**96.0**	84.0
	SVM	69.1	74.5	51.0
	KNN	45.2	48.0	36.0
	ANN	0.1	0.2	0.1
80-20	DNN	91.2	**94.0**	86.0
	SVM	71.1	72.4	69.7
	KNN	45.1	47.0	44.0
	ANN	0.5	0.2	0.1
70-30	DNN	95.0	**99.0**	92.0
	SVM	71.6	73.0	70.3
	KNN	44.0	46.1	42.0
	ANN	0.1	0.2	0.1
60-40	DNN	93.1	**97.0**	89.0
	SVM	70.5	71.8	68.1
	KNN	41.8	42.6	41.3
	ANN	0.1	0.2	0.1
50-50	DNN	93.0	**98.0**	91.0
	SVM	69.1	75.0	53.0
	KNN	40.4	41.2	40.3
	ANN	0.1	0.2	0.1

Table 5: Performance comparison of the propose DNN with SVM, KNN and ANN based on accuracy

Partition	Algorithms (%)	Mean (%)	Best (%)	Worst (%)
90-10	DNN	89.7	**96.0**	89.0
	SVM	84.1	86.6	75.4
	KNN	71.7	73.3	66.2
	ANN	5.0	5.0	5.0
80-20	DNN	91.3	**94.1**	86.2
	SVM	85.1	85.8	84.6
	KNN	72.0	72.6	71.4
	ANN	5.0	5.0	5.0
70-30	DNN	94.8	**98.7**	92.2
	SVM	85.4	86.1	84.8
	KNN	70.8	72.1	70.1
	ANN	5.0	5.0	5.0
60-40	DNN	93.2	**97.0**	89.2
	SVM	84.9	85.5	84.1
	KNN	70.3	70.7	70.1
	ANN	5.0	5.0	5.0
50-50	DNN	92.8	**97.6**	90.6
	SVM	84.1	84.4	83.8
	KNN	69.7	70.1	69.6
	ANN	5.0	5.0	5.0

Table 5 presents the accuracy of the DNN in authenticating the user of a mobile touch screen device in terms of keystroke dynamic. It is clearly indicated that the propose DNN has better accuracy than the compared algorithms.

Table 6: Performances comparison of the DNN with SVM, KNN and ANN based on FPR

Partition	Algorithms (%)	Mean (%)	Best (%)	Worst (%)
90-10	DNN	9.7	3.6	15.8
	SVM	0.5	**0.4**	0.9
	KNN	1.0	1.0	2.0
	ANN	2.5	1.8	3.5
80-20	DNN	8.5	5.8	13.6
	SVM	0.5	**0.5**	0.5
	KNN	1.0	1.0	1.0
	ANN	2.0	1.8.	2.3
70-30	DNN	5.3	1.6	7.6

	SVM	0.5	**0.5**	0.5
	KNN	1.0	1.0	1.0
	ANN	2.0	1.8.	2.3
60-40	DNN	6.7	3.0	10.6
	SVM	0.5	**0.5**	0.6
	KNN	1.0	1.0	1.0
	ANN	1.9	1.7	2.3
50-50	DNN	7.2	2.8	11.0
	SVM	0.6	**0.5**	0.6
	KNN	1.0	1.0	1.0
	ANN	1.8	1.7	2.2

Table 6 clearly indicates that in terms of the FPR, the SVM has the lowest FPR compared to the propose DNN. In this parameter, the DNN fails to outperform the classical algorithms.

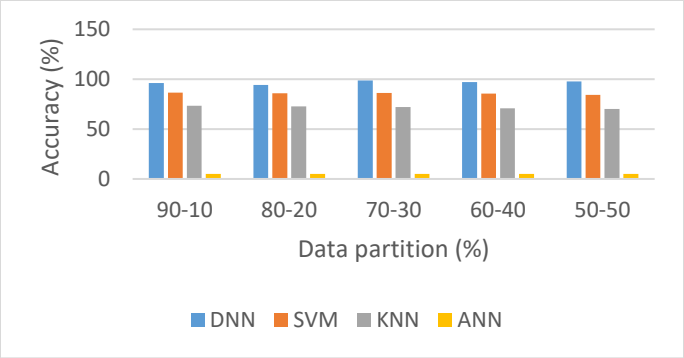

Figure 4: Overall accuracy rate of the proposed deep learning – DNN compared to the SVM, KNN and ANN

Figure 4 indicates that the DNN model has the best classification accuracy than the compared algorithms: SVM, KNN and ANN with ANN producing the worst classification accuracy based on the keystroke dynamics. Our proposed DNN model proves to be the overall best performing algorithm for classification based on the keystroke dynamic data providing the best accuracy rate. It indicates that the DNN model provides a high rate of correctly classified instances and maintaining a low rate of classifying incorrect instances.

Our research work provided a description of the application of DNN in authenticating users of mobile touch screen device based on keystroke dynamics. The authentication security system is to identify authentic users based on keystroke dynamics on mobile touch screen device. As a result, keystroke dynamic features were used for the training of the propose DNN without feature extraction with varying data partition ratios. The DNN authentication based on the keystroke dynamics was applied to classy users based on evaluation measures: f1-measure, recall, accuracy and FPR.

The feature extraction method that the classical algorithms heavily rely on for their performance in the modelling process is a multiple work and human intervention is required significantly. Our propose DNN approach for authentication based on keystroke dynamics is able to eliminate the double work of the feature extraction mostly practiced by researchers in the mobile touch screen device domain.

From the results presented in Tables 3 – 6 and Figure 4. It is clear that the propose DNN can perform better than the classical algorithms in terms of authenticating users of mobile touch screen devices based on keystroke dynamic. The recall and F1-measure values of the propose DNN for authentication based on keystroke dynamics ranges from 94 to 99% while accuracy ranges from 94 – 98.7%. The possible reason why the DNN performs better than the classical algorithms is because of the ability of the DNN to process large size of dataset without requiring feature extraction to discover intricate structures. The propose DNN has proven to provide better authentication of mobile touch screen device based on keystroke dynamic without feature extraction typically required by the classical algorithms. As such, the extra steps of feature extraction that is tedious and incurring extra computational processes can be eliminated with the propose DNN. The DNN has proven that it is a good algorithm with the required robustness to improve the security of the mobile touch screen devices. Therefore, mobile touch screen authentication system can be developed with the propose DNN to improve security of the mobile devices. The experimental result obtained from the study shows that the DNN is a choice algorithm for building classifier for the future research work on keystroke dynamic based user authentication.

The task of authenticating mobile touch screen device considered accuracy, F1-measure and recall as critical measures for evaluating the effectiveness of the authentication systems. The higher the value of these measures the better is the authentication system. The propose DNN authentication based on the keystroke dynamic can be considered to be successful because of its performance on the three performance measures. Though, the propose DNN has inferior performance on FPR compared to the classical algorithms regarding rejections - FPR. This means that the propose DNN can wrongly classify some few instances as the percentage is not much. It is argued that a classification technique is said to be good if the TPR is high while maintaining a low FPR [42]. Therefore, the propose deep learning - DNN is considered the best because the SVM does not maintain high TPR and low FPR like the deep learning – DNN classifier.

5. Conclusions and Future Work

In this paper, we proposed a deep learning approach to build a touch screen mobile phone authentication scheme based on keystroke dynamics. An experiment was carried out and the deep learning model was evaluated by comparing it with conventional machine learning algorithms: the SVM, KNN and ANN. Results of the experiment show that the propose deep learning model outperforms the compared algorithms. The results indicated the feasibility of using deep learning to improve the security system of the mobile smartphone touch screen devices. The deep learning approach has succeeded in eliminating the tedious feature extraction step required by the conventional algorithms: SVM, KNN and ANN. The propose dense DNN low performance on FPR which is considered to be the next future work to improve the value of the FPR. In the future, we plan to use behavioral biometric data extracted from users when drawing a pattern password.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

References

[1] M. Shahzad, A.X. Liu, A. Samuel, 'Secure unlocking of mobile touch screen devices by simple gestures - You can see it but you can not do it', in Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, 39–50, 2013, doi:10.1145/2500423.2500434.

[2] P. Studies, C. Science, 'ECG Authentication for Mobile Devices by Juan Sebastian Arteaga Falconi', **65(3)**, 591–600, 2013.

[3] M. Shahzad, A.X. Liu, A. Samuel, 'Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures', IEEE Transactions on Mobile Computing, **16**(10), 2726–2741, 2017, doi:10.1109/TMC.2016.2635643.

[4] T. Vu, A. Baid, S. Gao, M. Gruteser, R. Howard, J. Lindqvist, P. Spasojevic, J. Walling, 'Capacitive touch communication: A technique to input data through Devices' Touch Screen', IEEE Transactions on Mobile Computing, **13**(1), 4–19, 2014, doi:10.1109/TMC.2013.116.

[5] G. Li, P. Bours, 'Studying WiFi and accelerometer data based authentication method on mobile phones', in ACM International Conference Proceeding Series, 43–49, 2018, doi:10.1145/3230820.3230824.

[6] M. Ernst, T. Swan, V. Cheung, A. Girouard, 'Typhlex: Exploring Deformable Input for Blind Users Controlling a Mobile Screen Reader', IEEE Pervasive Computing, **16**(4), 28–35, 2017, doi:10.1109/MPRV.2017.3971123.

[7] J. Lai, D. Zhang, 'ExtendedThumb: A target acquisition approach for one-handed interaction with touch-screen mobile phones', IEEE Transactions on Human-Machine Systems, **45**(3), 362–370, 2015, doi:10.1109/THMS.2014.2377205.

[8] R. Francese, M. Risi, G. Tortora, M. Tucci, 'Visual Mobile Computing for Mobile End-Users', IEEE Transactions on Mobile Computing, **15**(4), 1033–1046, 2016, doi:10.1109/TMC.2015.2422295.

[9] J. Yu, H. Han, H. Zhu, Y. Chen, J. Yang, Y. Zhu, G. Xue, M. Li, 'Sensing human-screen interaction for energy-efficient frame rate adaptation on smartphones', IEEE Transactions on Mobile Computing, **14**(8), 1698–1711, 2015, doi:10.1109/TMC.2014.2352862.

[10] D. Kunda, M. Chishimba, 'A Survey of Android Mobile Phone Authentication Schemes', Mobile Networks and Applications, 1–9, 2018, doi:10.1007/s11036-018-1099-7.

[11] X. Zhao, T. Feng, W. Shi, I.A. Kakadiaris, 'Mobile user authentication using statistical touch dynamics images', IEEE Transactions on Information Forensics and Security, **9**(11), 1780–1789, 2014, doi:10.1109/TIFS.2014.2350916.

[12] N. Wakabayashi, M. Kuriyama, A. Kanai, 'Personal authentication method against shoulder-surfing attacks for smartphone', in 2017 IEEE International Conference on Consumer Electronics, ICCE 2017, 153–155, 2017, doi:10.1109/ICCE.2017.7889266.

[13] W. Meng, W. Li, D.S. Wong, J. Zhou, 'TMGuard: A touch movement-based security mechanism for screen unlock patterns on smartphones', in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 629–647, 2016, doi:10.1007/978-3-319-39555-5_34.

[14] W. Meng, Y. Wang, D.S. Wong, S. Wen, Y. Xiang, 'TouchWB: Touch behavioral user authentication based on web browsing on smartphones', Journal of Network and Computer Applications, **117**, 1–9, 2018, doi:10.1016/j.jnca.2018.05.010.

[15] M. Gao, X. Hu, B. Cao, D. Li, 'Fingerprint sensors in mobile devices', in Proceedings of the 2014 9th IEEE Conference on Industrial Electronics and Applications, ICIEA 2014, 1437–1440, 2014, doi:10.1109/ICIEA.2014.6931394.

[16] K. Cao, A.K. Jain, Hacking Mobile Phones Using 2D Printed Fingerprints, 2016.

[17] E. Vazquez-Fernandez, D. Gonzalez-Jimenez, 'Face recognition for authentication on mobile devices', Image and Vision Computing, **55**, 31–33, 2016, doi:10.1016/j.imavis.2016.03.018.

[18] W. Meng, W. Li, L. Jiang, J. Zhou, 'SocialAuth: Designing touch behavioral smartphone user authentication based on social networking applications', in IFIP Advances in Information and Communication Technology, 180–193, 2019, doi:10.1007/978-3-030-22312-0_13.

[19] S. Alotaibi, A. Alruban, S. Furnell, N. Clarke, 'A novel behaviour profiling approach to continuous authentication for mobile applications', in ICISSP 2019 - Proceedings of the 5th International Conference on Information Systems Security and Privacy, 246–251, 2019, doi:10.5220/0007313302460251.

[20] M. Ehatisham-ul-Haq, M. Awais Azam, U. Naeem, Y. Amin, J. Loo, 'Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing', Journal of Network and Computer Applications, **109**, 24–35, 2018, doi:10.1016/j.jnca.2018.02.020.

[21] P. Kumar, R. Saini, P. Pratim Roy, D. Prosad Dogra, 'A bio-signal based framework to secure mobile devices', Journal of Network and Computer Applications, **89**, 62–71, 2017, doi:10.1016/j.jnca.2017.02.011.

[22] M. Smith-Creasey, F.A. Albalooshi, M. Rajarajan, 'Continuous face authentication scheme for mobile devices with tracking and liveness detection', Microprocessors and Microsystems, **63**, 147–157, 2018, doi:10.1016/j.micpro.2018.07.008.

[23] B. Kolosnjaji, A. Hufner, C. Eckert, A. Zarras, 'Learning on a Budget for User Authentication on Mobile Devices', in ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2042–2046, 2018, doi:10.1109/ICASSP.2018.8461898.

[24] L. Wang, K. Huang, K. Sun, W. Wang, C. Tian, L. Xie, Q. Gu, 'Unlock with Your Heart', Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, **2**(3), 1–22, 2018, doi:10.1145/3264950.

[25] J.M. de Fuentes, L. Gonzalez-Manzano, A. Ribagorda, 'Secure and usable user-in-a-context continuous authentication in smartphones leveraging non-assisted sensors', Sensors (Switzerland), **18**(4), 2018, doi:10.3390/s18041219.

[26] Y. Song, Z. Cai, Z.L. Zhang, 'Multi-touch Authentication Using Hand Geometry and Behavioral Information', in Proceedings - IEEE Symposium on Security and Privacy, 357–372, 2017, doi:10.1109/SP.2017.54.

[27] L. Zhou, Y. Kang, D. Zhang, J. Lai, 'Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones', Decision Support Systems, **92**, 14–24, 2016, doi:10.1016/j.dss.2016.09.007.

[28] C. Bo, L. Zhang, X.Y. Li, Q. Huang, Y. Wang, 'SilentSense: Silent user identification via touch and movement behavioral biometrics', in Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, ACM Press, New York, New York, USA: 187–189, 2013, doi:10.1145/2500423.2504572.

[29] U. Burgbacher, K. Hinrichs, 'An implicit author verification system for text messages based on gesture typing biometrics', in Conference on Human Factors in Computing Systems - Proceedings, 2951–2954, 2014, doi:10.1145/2556288.2557346.

[30] Y. Chen, J. Sun, R. Zhang, Y. Zhang, 'Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices', in Proceedings - IEEE INFOCOM, 2686–2694, 2015, doi:10.1109/INFOCOM.2015.7218660.

[31] H. Xu, Y. Zhou, M.R. Lyu, 'Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones', 187–198, 2014.

[32] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, 'Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication', IEEE Transactions on Information Forensics and Security, **8**(1), 136–148, 2013, doi:10.1109/TIFS.2012.2225048.

[33] P. Saravanan, S. Clarke, D.H. Chau, H. Zha, 'LatentGesture: Active user authentication through background touch analysis', in ACM International Conference Proceeding Series, 110–113, 2014, doi:10.1145/2592235.2592252.

[34] F. He, L. Bao, R. Wang, J. Li, D. Xu, X. Zhao, 'A multimodal deep architecture for large-scale protein ubiquitylation site prediction', in Proceedings - 2017 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2017, 108–113, 2017.

[35] Y. Lecun, Y. Bengio, G. Hinton, Deep learning, Nature, **521**(7553), 436–444, 2015, doi:10.1038/nature14539.

[36] M.A. Wani, F.A. Bhat, S. Afzal, A.I. Khan, Introduction to Deep Learning, 1–11, 2020, doi:10.1007/978-981-13-6794-6_1.

[37] Y. Liang, Z. Cai, J. Yu, Q. Han, Y. Li, 'Deep Learning Based Inference of Private Information Using Embedded Sensors in Smart Devices', IEEE Network, **32**(4), 8–14, 2018, doi:10.1109/MNET.2018.1700349.

[38] L. Sun, Y. Wang, B. Cao, P.S. Yu, W. Srisa-An, A.D. Leow, 'Sequential Keystroke Behavioral Biometrics for Mobile User Identification via Multi-view Deep Learning', in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 228–240, 2017, doi:10.1007/978-3-319-71273-4_19.

[39] Y. Deng, Y. Zhong, Keystroke Dynamics Advances for Mobile Devices Using Deep Neural Network, 59–70, 2015, doi:10.15579/gcsr.vol2.ch4.

[40] M. Rampurawala, Classification with TensorFlow and Dense Neural Networks, Heart Beat, 2019.

[41] B. Zheng, S.W. Yoon, S.S. Lam, Y. Xiang, Y. Zhou, H. Liu, W.-L. Xiang, M.-Q. An, B. Subanya, P.G. Scholar, K. Srinivas, G.R. Rao, A.Govardhan, S. Shilaskar, A. Ghatol, E. Rashedi, H.N. Saeid, H. Nezamabadipour, K. Polat, G. Salih, D. Pal, K.M. Mandana, S. Pal, D. Sarkar, C. Chakraborty, H.S.N. Murthy, M.Meenakshi, R.A. Mohammadpour, S.M. Abedi, et al.,

Machine Learning Repository, Computers and Operations Research,Elsevier, **40**(November), 21–22, 2015.

[42] A.A. Bello, H. Chiroma, A.Y. Gital, L.A. Gabralla, S.M. Abdulhamid, L. Shuib, 'Machine learning algorithms for improving security on touch screen devices: a survey, challenges and new perspectives', Neural Computing and Applications, 2020, doi:10.1007/s00521-020-04775-0.

[43] A. De Luca, A. Hang, F. Brudy, C. Lindner, H. Hussmann, 'Touch me once and i know it's you! Implicit authentication based on touch screen patterns', in Conference on Human Factors in Computing Systems - Proceedings, 987–996, 2012, doi:10.1145/2207676.2208544.