Person Authentication by Gait Data from Smartphone Sensors Using Convolutional Autoencoder

Ashika Kothamachu Ramesh, Kavya Sree Gajjala, Kotaro Nakano, Basabi Chakraborty

Person Authentication by Gait Data from Smartphone Sensors using Convolutional Autoencoder

Kothamachu Ramesh Ashika[1], Gajjala Kavya Sree[1], Kotaro Nakano[2], and Basabi Chakraborty[3]

[1] Graduate School of Software and Information Science, Iwate Prefectural University,Takizawa, Iwate,Japan.
[2] Research and Regional Co-operative Divison, Iwate Prefectural University,Takizawa, Iwate, Japan.
[3] Faculty of Software and Information Science, Iwate Prefectural University, Takizawa, Iwate, Japan.

Abstract. Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify who he or she is. Human gait serves as an important non invasive biometric modality for an authentication tool in various security applications. Recently due to increased use of smartphones and easy capturing of human gait characteristics by embedded smartphone sensors, human gait related activities can be utilized to develop user authentication model. In this work, a new method for user authentication from smartphone sensor data by a hybrid deep network model named convolutional autoencoder has been proposed and the performance of the model is compared with other machine learning including deep learning based techniques by simulation experiments with bench mark data sets. It is found that our proposed authetication method from smartphone sensor data with convolutional autoencoder reduces the time for authentication and also produces fair authentication accuracy and EER. It can be potentially used for person authentication in real time.

Keywords: Biometric authentication · smartphone sensors · human gait· convolutional autoencoder .

1 Introduction

With increasing demands of user identification or authentication[1] for secured processing of today's big data and artificial intelligence based applications, biometric techniques play a major role. The biometric traits that are commonly used in different systems are face [2], fingerprints, palm print, handwriting, iris, gait, voice etc. Among them, gait recognition is a relatively new behavioral biometric technique which aims to recognize the person by the way they walk without intruding the persons privacy. It can be used in applications for criminal detection or for health monitoring to diagnose the abnormal walking that led to health issues. Every individual has unique walking style by which a person can

be differentiated and identifed[3]. Authentication by gait can be carried out by extracting some salient properties related to the coordinated cyclic motions.

Smart devices are now equipped with top quality sensors, fast processing and communication power. User authentication based on gait characteristics captured by embedded smartphone sensors is one of the most active mode of biometrics for smartphone based security applications. The rapidly evolving field of wireless communication allows us to record the time series data from smartphone sensors without any hassle to the user [4]. Human activity recognition from smartphone sensor data is also an active research area because of its importance in health care and assisted living. Activity dependent authentication framework based on human gait characteristics from smartphone sensor data has been proposed by one of the authors in earlier works [17] [25].

In recent years, machine learning including deep learning techniques has evolved a lot and increasingly applied to classification problems. Deep neural networks (DNN), especially Convolutional Neural Networks (CNN) have been proposed in many research works for user authentication. In this work, we have proposed an authentication approach using a new hybrid DNN model which is a combination of CNN and autoencoders (convolutional autoencoders) to reduce the time of authentication as well as to increase accuracy of authentication. We have performed simulation experiments with the proposed model by a few benchmark datasets and found that our model works better when compared with traditional machine learning or other deep learning models. In the next section brief description of related works on person authentication is presented followed by the outline of the proposed method in the following section. The next section contains simulation experiments and results and the last section is summarization and conclusion.

2 Related Work

In this modern world, almost everyone is dependent on smartphone for daily activities like connecting friends and relatives across the globe or managing personal obligations from monitoring health to paying bills online. Smartphones have in built motion sensors like accelerometer, gyroscope, magnetometer. Accelerometers can measure any movement of the phone while gyroscope can capture current orientation of the phone in all three axes (X, Y, and Z).Three dimensional time series data are generated from accelerometer and gyroscope.Time series is a sequence of data that describes the change of the observed phenomenon over time. Data from motion sensors of smartphone capture gait characteristics of the user carrying the phone. Sensors attached to fixed body positions are also capable of capturing gait characteristics but the popularity of smartphones motivates development of smartphone based authentication applications using gait characteristics[5] [21]. Inertia based gait recognition is popular because it can analyze the details of movement characteristics [6]. An efficient higher order statistical analysis based gait person authentication which is able to operate on multichannel and multisensor data by combining feature-level and sensor-level fusion is explained in [7].

Recently deep neural networks (DNN) are found to be very efficient at delivering high quality results in pattern classification problems. A review of research works on human activity recognition by motion data from inertial sensors using deep learning is found in [8]. Among DNN models, CNN produce good results for many classification problems. Gait classification and person authentication using CNN is presented in [9]. Another deep recurrent network model, Long Short Term Memory (LSTM) is also suitable for analysis of sensor data for recognition. Person authentication from gait data during human activity with smartphone sensors using LSTM is explained in[10]. A good comprehensive study of the research work on authentication of smartphone users with behavioral biometric can be found in [11]. Different kinds of user authentication techniques are also explained in [12]. A comparative analysis of hybrid deep learning models for human activity recognition is considered in [13]. Unobtrusive user authentication on mobile phones using biometric gait recognition is presented in [14]. Authentication of smartphone user using behavioral biometrics is explained in [15]. The use of autoencoders for gait-based person authentication is found in [16]. For lowering computational cost of classifier, knowledge distillation is used as an approach for designing low cost deep neural network based biometric authentication model for smartphone user in [17].

3 Proposed Method and Comparative study

In this work, person authentication approach by gait characteristics captured from smartphone sensor data is proposed with Convolutional Autoencoder (CAE), a new hybrid deep network model to reduce the time of authentication as well as to increase the accuracy. Convolutional autoencoders are usually popular in computer vision or in image analysis. Convolutional autoencoder along with LSTM has also been used in [18] for time series prediction. In authentication problem, CAE used to extract features for finger vein verification problem along with SVM (Support Vector Machine) for classification in [19]. The use of CAE in radar based classification of human activities shows promising improvement over SVM classifiers in [20]. Deployment of CAE for smartphone sensor based data analysis in user authentication has not been addressed yet.

This work aims to exploit CAE for analysing smartphone sensor data for person authentication. The performance of convolutional autoencoder based authentication method is evaluated by simulation experiments with bench mark data sets and a comparative study with other popular deep network models for person authentication has also been done. A brief introduction of CAE and other DNN models used in our study is presented in the next subsections.

3.1 Convolutional Autoencoder (CAE)

Convolutional Autoencoder is a combination of auto encoder and convolutional neural network. Autoencoders are neural networks that can be easily trained on any kind of input data. Generally encoders compress the given input into fixed dimension and decoder transforms the code into original input. In convolutional autoencoder, encoding and decoding use convolution and deconvolution,

the encoder use the convolutional layer, batch normalization layer, an activation function and at last, a maxpooling function which reduces the dimensions of the feature maps. When encoder is complete, the feature maps are flattened and a dense layer is used for latent space representation and the deconvolution is used for upsampling of the incoming feature maps followed by batch normalization and activation function.

3.2 Deep Neural Network Models used for Comparison

Convolutional Neural Networks (CNN) CNN is the most popular deep neural network model which has become dominant in various computer vision tasks. CNN is composed of multiple building blocks, such as convolution layers, pooling layers, and fully connected layers, and it is designed to automatically and adaptively learn spatial hierarchies of features.

Long short term memory (LSTM) and Bi directional long short term memory(BiLSTM) Long short term memory (LSTM) is a special kind of Recurrent Neural Network (RNN), capable of learning spatial dependencies. They have internal mechanisms called gates (input gate, output gate, forget gate) that can regulate flow of information and can learn data in a sequence. Another core concept of LSTM is the cell state that acts like memory of the network that transfers relative information all the way in the sequence chain. Bidirectional LSTM is an extension of LSTM that can improve model performance on classification problems. BiLSTMs are combination of two LSTMs one fed with data sequence in normal time order and other fed in reverse time order. The outputs of the two networks are then concatenated at each time step.

Gated Recurrent Unit (GRU) and Bidirectional Gated Recurrent Unit (BiGRU) GRU is an improved version of standard recurrent neural network similar to LSTM that aims to solve vanishing gradient problem. Main advantage of GRU is that it can be trained to keep the information from long back without removing it through time or information which is irrelevant to the prediction. As they have few operations, they are little speedier to train. BiGRU is combination of two GRUs one working on normal time order and the other one on reverse time order.

4 Simulation Experiments and Results

Simulation experiments with several bench mark datasets have been done to evaluate the eficiency of convolutional autoencoder in person authentication from smartphone sensor data. For comparison, several other deep learning methods have been used along with some popular traditional machine learning (ML) techniques such as k-nearest neighbour (KNN), Naive Bayes (NB), Support Vector Machine (SVM) and Linear Discriminant Analysis (LDA). In the next subsections, the data sets and simulation results are presented.

4.1 Datasets

1. WISDM(Wireless Sensor Data Mining)
   Smartphone is used to collect the data of 6 activities WALKING, JOGGING, UPSTAIRS, DOWNSTAIRS, SITTING, and STANDING from 36 subjects carrying their mobile device in front leg pocket. There are 1,098,207 samples available in the dataset which are sampled at 20Hz, 46 statistical measure like standard deviation, average absolute difference etc. are used. The details can be found in [22].
2. UCI-HAR data set
   Data of 30 volunteers within age limit of 19-48 are considered, each person performed six activities (WALKING, WALKINGUPSTAIRS, WALKING-DOWNSTAIRS, SITTING, STANDING, LAYING) wearing a smartphone on the waist. It consists of 748406 samples captured at the rate of 50HZ. The sensor signals were preprocessed applying noise filters and sampled in 2.56 sec fixed sliding window and 50 percent overlap and all the features are normalized and bounded within [-1,1]. The details are found in [23].
3. Motion sensor data set
   Data generated by accelerometer and gyroscope sensors with an iPhone 6s kept in the front pocket is collected from 24 persons of 6 activities in 15 trials in the same environment conditions (DOWNSTAIRS, UPSTAIRS, WALKING, JOGGING, SITTING, AND STANDING). This data set is obtained from Queen Mary University of London's repository. The details are in [24].

4.2 Simulation Results

In this section the performance of all the models are evaluated from the simulation results. Classification accuracy, elapsed time, true positive rate (TPR), false positive rate (FPR) and equal error rate (EER) are used to analyze the performance of the models.

Table 1. Authentication accuracies of various models

Accuracies of models (in percentage)			
Classifiers	WISDM	UCIHAR	Motion Sense
KNN	0.44	0.65	0.56
Naive Bayes	0.36	0.59	0.62
SVM	0.46	0.68	0.49
LDA	0.53	0.78	0.74
RF	0.90	0.86	0.80
LSTM	0.66	0.88	0.77
BiLSTM	0.93	0.89	0.81
GRU	0.63	0.80	0.80
BiGRU	0.96	0.90	0.90
CNN	0.98	0.90	0.94
CONV AUTOENCODER	**0.995**	**0.936**	**0.971**

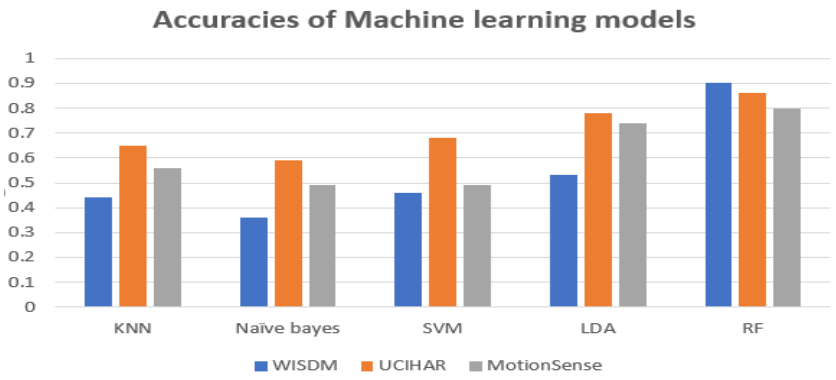

Fig. 1. Authentication accuracies of machine learning models.

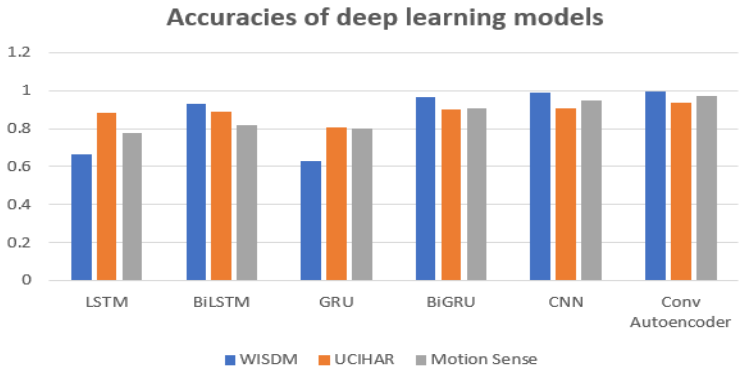

Fig. 2. Authentication accuracies of deep learning models.

Table1 represents authentication accuracies of different machine learning models for different datasets.It seems that all the deep network based models perform better than traditional ML methods. Figure 1 and Figure 2 present the comparative results of authentication accuracy for all the data sets by traditional ML methods and DNN based methods respectively. From the figures it can be seen that RF produces the best accuracy among ML methods for all the data sets while proposed CAE based authentication method produces the best accuracy among deep networks based models though CNN and BiGRU also produce high accuracy. As the input data is utilized twice for training in BiLSTM, it has additional training capability and it outperformed LSTM regarding accuracy though it takes longer time. LSTM is comparatively fast but each hidden state has been computed until the previous hidden state computation is complete, training takes a lot of resources and it impacts the accuracy of the model.

BiGRU also have same ability to keep memory from previous activations like LSTM but it performs both input and forget gates operation together with its reset gate, so it has fewer tensor operations and it is speedier than LSTM and BiLSTM while producing better accuracy for authentication.

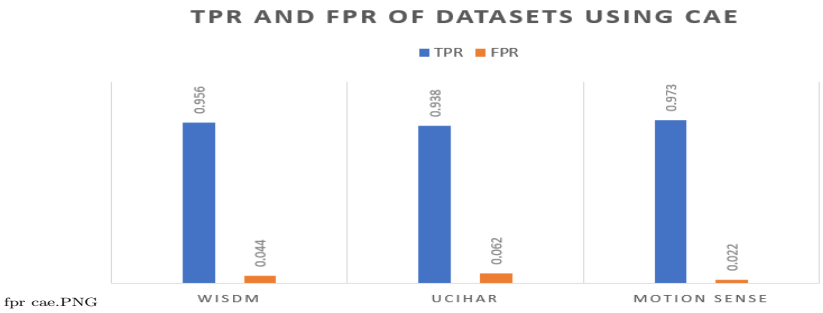

Fig. 3. TPR and FPR of datasets by using CAE

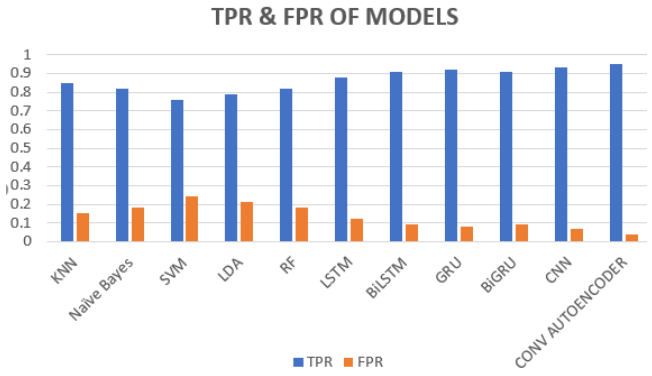

Fig. 4. TPR & FPR of different authentication models

Figure 3 represents TPR and FPR of our proposed CAE based authentication results for all the data sets while Figure 4 represents TPR, FPR of all other models for WISDM dataset. It is found that deep network based models perform comparatively better than other models with high TPR and low FPR for WISDM data sets. Other data sets also produce similar results. Among all the models, CAE seems to be the best and CNN is the second best in terms of TPR and FPR.

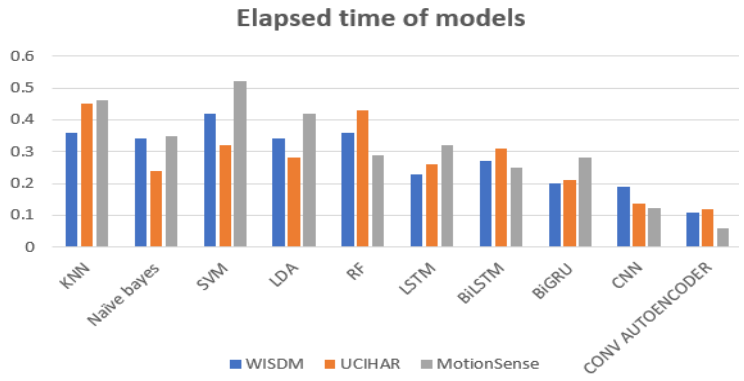

Fig. 5. Time taken for authentication in secs

For better authentication of a person, processing time also plays a key role. Less processing time represents, it can be potentially used for real time authentication of a person. Figure 5 presents authentication time taken by each model for each of the data sets. It is found that the proposed convolutional autoencoder based model is the fastest compared to the other models for all the data sets. Time taken for authentication by CAE seems sufficiently low to implement in real time on smartphone. EER of deep learning models are shown in Table 3. It is seen that CNN and GRU gives good EER values for WISDM and UCIHAR dataset. Low EER values represents that particular model authenticates person efficiently. Convolutional Autoencoder based proposed model produces the best EER values for all the data sets.

Table 2. Equal Error Rate (EER) of deep learning models

EER of deep learning models			
Classifiers	WISDM	UCIHAR	Motion Sense
LSTM	2.74	3.24	2.50
BiLSTM	2.14	3.31	3.82
GRU	1.80	2.45	2.78
BiGRU	4.41	4.25	3.12
CNN	1.92	2.95	2.10
CONV AUTOENCODER	**1.12**	**2.14**	**1.74**

5 Summarization and Conclusion

Person authentication with smartphone sensor data utilizing human gait characteristics by deep neural network model has been studied in this work. The ca-

pability of a convolutional autoencoder, a hybrid deep network model previously used in computer vision and image analysis, has been examined and proposed as a suitable candidate for person authentication by gait characteristics captured by smartphone sensor data. The performance of the proposed authentication method has been evaluated by simulation experiments with benchmark datasets and also compared with several traditional machine learning approaches as well as popular deep neural network based methods. It is found that all the deep network models perform better than traditional machine learning classifiers as they are capable of extracting proper features implicitly.

Proposed convolutional autoencoder based model gives the best accuracy in less processing time for all the data sets among all deep neural network based models. It is also found that the proposed CAE based model has the potential for development of real time smartphone based person authentication application. There are many limitations for gait authentication of a person like dressing style or if a person met with an accident walking style of the person changes and also depends on the environment persons walking style changes. So in the future work we will consider all the limitations and apply these techniques for accurate authentication in real time. As convolutional autoencoder yields good results for authentication, by applying continuous authentication techniques and transfer learning approach on this model, it can be a good candidate for developing smartphone based continuous person authentication for health care applications for elderly people.

References

1. A. N. Kataria, D. M. Adhyaru, A. K. Sharma and T. H. Zaveri, "A survey of automated biometric authentication techniques," Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, pp. 1-6, (2013) doi: 10.1109/NUiCONE.2013.6780190.
2. M. Zulfiqar, F. Syed, M. J. Khan and K. Khurshid, "Deep Face Recognition for Biometric Authentication," International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, pp. 1-6, (2019)doi: 10.1109/ICECCE47252.2019.8940725.
3. J. Lu, G. Wang, and P. Moulin, "Human identity and gender recognition from gait sequences with arbitrary walking directions," IEEE Transactions on Information Forensics and Security, vol. 9(1), pp.51-61, 2014.
4. T. B. Singha, R.K. Nath and A.V. Nasimhadhan, "Person Recognition using Smartphones' Accelerometer data",https://arxiv.org/pdf/1711.04689, 2017.
5. M. Nixon, T. Tan, and R. Chellappa, "Human identification based on gait," Springer, 2006.
6. S Sprager, MB Juric. Inertial Sensor-Based Gait Recognition: A Review. Sensors (Basel). 2015 Sep 2;15(9):22089-127. doi: 10.3390/s150922089.
7. S. Sprager and M. B. Juric, "An efficient HOS based gait authentication of accelerometer data," IEEE Transactions on Information Forensics and Security, Vol. 10(7), pp. 1486-1498, 2015.
8. K. Chen, D. Zhang, L. Yao et.al., "Deep Learning for Sensor-based Human Activity Recognition: Overview, Challenges and Opportunities" 2018. https://arxiv.org/abs/2001.07416

9. Yuan W., Zhang L., " Gait Classification and Identity Authentication Using CNN". In: Li L., Hasegawa K., Tanaka S. (eds) Methods and Applications for Modeling and Simulation of Complex Systems. AsiaSim 2018. Communications in Computer and Information Science, vol 946.
10. M. Zhang, "Gait Activity Authentication Using LSTM Neural Networks with Smartphone Sensors," 15th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), Shenzhen, China, 2019, pp. 456-461, doi: 10.1109/MSN48538.2019.00092.
11. A.Mahfouza, T.M. Mahmoud and A.S. Eldin, "A survey on Behavioural Biometric Authentication on Smartphones", Journal of Information Security and Applications, vol 37, pp.28-37, Dec 2017.
12. E U H Muhammad,A M Awais,L Jonathan, et al., "Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing. Sensors, Vol.17(9),pp.2043-2074, 2017.
13. S. Abbaspour;F. Fotouhi;A. Sedaghatbaf; H. Fotouhi;M. Vahabi;M. Linden, "A Comparative Analysis of Hybrid Deep Learning Models for Human Activity Recognition.", Sensors , Vol. 20(19) , 2020.
14. M.O. Derawi;C. Nickely;P. Bours;C. Busch "Unobtrusive user authentication on mobile phones using Biometric gait recognition. Proc. 6th International conference on intelligent Information Hiding and Multimedia signal processing, Germany, Oct, pp. 306-311, 2010
15. A. Alzubaidi and J. Kalita, Authentication of Smartphone users using Behavioral Biometrics, Journal of IEEE Communications Surveys and Tutorial, Vol. 8, Issue 3, pp. 1998-2026, 2015.
16. Cheheb, N. Al-Maadeed, S. Al-Madeed and A. Bouridane, "Investigating the Use of Autoencoders for Gait-based Person Recognition," 2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Edinburgh, pp. 148-151, 2018.
17. B. Chakraborty, K. Nakano, Y. Tokoi and T. Hashimoto, "An Approach for Designing Low Cost Deep Neural Network based Biometric Authentication Model for Smartphone User," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, pp. 772-777, 2019.
18. X. Zhao, X. Han, W. Su and Z. Yan, "Time series prediction method based on Convolutional Autoencoder and LSTM," Chinese Automation Congress (CAC), Hangzhou, China, pp. 5790-5793, 2019.
19. B. Hou and R. Yan, "Convolutional Autoencoder Model for Finger-Vein Verification," in IEEE Transactions on Instrumentation and Measurement, vol. 69(5), pp. 2067-2074, May 2020.
20. M. S. Seyfioğlu, A. M. Özbayoğlu and S. Z. Gürbüz, "Deep convolutional autoencoder for radar-based classification of similar aided and unaided human activities," in IEEE Transactions on Aerospace and Electronic Systems, vol. 54(4), pp. 1709-1723, 2018.
21. D. Gafurov, K. Helkala, and T.Sondrol, "Biometric gait authentication using accelerometer sensor," Journal of Computers, vol. 1(7), pp.51-59, 2006.
22. Wisdm dataset is publicly available in https://www.cis.fordham.edu/wisdm/dataset.php
23. https://archive.ics.uci.edu/ml/datasets/human+activity+recognition+using+smartphones
24. https://www.kaggle.com/malekzadeh/motionsense-dataset
25. B. Chakraborty, "Gait Related Activity Based Person Authentication with Smartphone sensors", Proc. 2018 12th International Conference on sensing Technology (ICST), pp.208-212, 2018.