IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

# Feasibility of Predicting Soft Biometric Traits Based on Keystroke Dynamics Characteristics

**Soumen Roy [1*], Utpal Roy [2], D. D. Sinha[3]**

[1]Dept. of Computer Science and Engineering, University of Calcutta, 92 APC Road, Calcutta -700 009, India
[2]Dept. of Computer & System Sciences, Visva-Bharati, Santiniketan -731235, India

[*]*Corresponding Author: soumen.roy_2007@yahoo.co.in*

**Available online at: www.ijcseonline.org**

***Abstract*—** This study investigates the feasibility of identifying age group, gender, handedness and number of hand(s) used of a user by measuring the typing pattern on a computer keyboard which has good impact on keystroke dynamics biometric user authentication system. Fuzzy-Rough Nearest Neighbour (FRNN) with the help of Vaguely Quantified Rough Set (VQRS) machine learning method was used to develop the model based on the collected typing pattern and evaluated the effectiveness of the classifier in this domain. Multiple benchmark datasets have been used to validate the proposed model in order to check the robustness of the proposed approach. The obtained results indicate that age group, gender, handedness, and a number of hand(s) used can be predicted by the way user type on a computer keyboard for a single predefined text. It is also observed that incorporation of such soft biometric traits as extra features with primary keystroke dynamics characteristics can be used to enhance the performance of keystroke dynamics systems pretending to be used in future at low cost. The model is developed with a limited number of samples collected from a small group of participants in a controlled environment. However, this model will be further trained and evaluated by some extra features which are easily available in each smartphone such as gyroscope and acceleration information. Identifying such traits are important issues in digital forensics, age-based access control, targeted advertisement and auto profiling of the users. It adopts a suitable method to be used on the desktop computer as well as a smartphone.

***Keywords*—** Keystroke Dynamics (KD), Soft Biometric, Fuzzy Rough NN (FRNN), Vaguely Quantified Rough Set (VQRS)*Introduction*

## I. INTRODUCTION

Knowledge-based authentication (PIN, Password, Graph pattern analysis) is the cheapest access control mechanism generally used in e-mail services, social network services, storage services, application services, web hosting services, TV services,…). But nowadays, this mechanism is not limited. It is combined with keystroke dynamics characteristics resulting in a more secure, stricter and stronger access control mechanism. Keystroke dynamics or recognizing typing style promises a parameter like behavioral biometric characteristics what we have learned in our life relates the disputes in existing knowledge-based user identity verification. This is the characteristics by which a user can be recognized by the way they type on a conventional computer keyboard or touchscreen, same as handwriting recognition. As behavioral biometric characteristics, the accuracy level of keystroke dynamics biometrics in user recognition is not promising with the others behavioral biometric characteristics such as signature, voice print, and gait recognition. The overall performance of the keystroke dynamics user recognition method is not acceptable due to several problems in data acquisition method which decreases the widespread use of this technique in real life applications. Where the acceptability of others behavioral biometrics are higher. In order to realize the fact and importance, it is highly essential to detect the issues and probable solutions to address the disputes associated with it.

Some of few studies have been conducted and suggested various methods to address the issues. A study [1] recommended that multiple tries in one session during data acquisition get the reliable typing pattern. Another study [2] suggested that biometric template updating decreases the error rate in the future. A study [3] recommended that score fusion of Gaussian Probability Function and Direction Similarity Measure increases the performance. The inclusion of soft biometrics trait gender with primary biometric characteristics increases the performance of the keystroke dynamics user recognition system suggested by a study [4]. However, keystroke dynamics in the present form cannot meet the European standard for access control system. The soft biometric traits are the physical and behavioral biometric characteristics extracted from the way of the type which has no promising user selective control but can be used to search the genuine user more time efficiently and accurately. As per a study [5], the authors explained that soft biometric traits are height, weight, gender, ethnicity, skin color, hair color, eye color of the user in face recognition. But as per the new definition of a study [6], the authors declared that soft biometric traits are body shape, cloth type, cloth color, accessories of the user along with the other definition in face recognition.

Some additional information about the user can significantly improve the user recognition performance in biometric systems [7]. As per the literature, gender information can be extracted from the way of typing a short text[4], the study obtained the accuracy of 91% to discriminate the gender on GREYC keystroke dynamics dataset created by them. They have used Support Vector Machine (SVM) as a classifier; they also reported that 20% of gain accuracy can be achieved by incorporation of only gender information as an additional feature. Idrus et al. [8] showed that it is possible to identify the gender (male/female), age group (<30≤ and <32≤), handedness (left handed/right handed) and hand(s) (one or both hands) used while typing and they reported the accuracy rate very close to 90%. Uzun et al. [9] showed that it is possible to identify the child group and adults users through typing pattern and they obtained the accuracy of more than 90% for the simple familiar Turkish text. They have used 13 classification algorithms where SVM (Linear) is achieved minimum Equal Error Rate for familiar text but the performance is not consistent with the other type of texts. A study [10] showed that the emotional state of an individual can be predicted by the way of typing on a computer keyboard. Jain et al. in 2004 [7] gained 5% of improvement for fingerprint recognition system incorporation of ethnicity (Asian/non-Asian), gender (male/female) and height in addition. The incorporation of body weight measurement and boy fat percentage as additional information decreases the error rate from 3.9% to 1.5% for fingerprint recognition system as per the study Ailisto et al. in 2006 [11]. Jain and Park in 2009 [12] enabled fast search technique in the facial image using freckles, moles and scares as additional information. Li et al. in 2009 [13] achieved the performance improvement of 40% to 50% for face recognition by the inclusion of gender in addition. Roy et al. in 2017 [14] reported that child user can be identified by their typing pattern on a convention keyboard as well as a touchscreen phone.

Table 1. Impact of incorporation of soft biometric traits with primary biometric characteristics

| Study | Biometric Modalities | Soft Biometric Traits | Accuracy Achieved | Impact |
|---|---|---|---|---|
| [15] | Faceprints | Gender and age | - | Used to search efficiency |
| [16] | Faceprints | Ethnicity | 92% | Automatically extracts the ethnicity and gender from face prints |
| | | Gender | 96% | |
| [17] | Fingerprints | Ethnicity | 96.3% | Enhances 5% of fingerprints recognition accuracy rate |
| | | Gender | 89.6% | |
| [18] | Faceprints | Ethnicity | 96.3% | Automatically extract the ethnicity information from face prints |
| [19] | Fingerprints | Body weight | 89% | Enhances 3.9% to 1.5% of fingerprints recognition accuracy rate |
| | | body fat | 65% | |
| [20] | Faceprints | Freckles, moles, scars on the face | - | Speed up the face recognition process |
| [4] | Keystroke Dynamics | Gender | 91% | Enhances 20% accuracy in keystroke dynamics user authentication system |

These previous experiments showed that incorporation of soft biometric information with the primary biometric characteristics improve the performance of biometric techniques in accuracy and time efficiency. Impact of identifying traits and incorporation of this score in user recognition in face print, fingerprint, and keystroke dynamics analysis are summarized in Table 1.A study [21] has been conducted to improve the evaluation performance of identifying soft biometric traits so that this technique can be used in real life applications. Machine learning techniques as a classification and evaluation method are common in keystroke dynamics domain in identifying soft biometric traits. But the performance of machine learning methods proposed to keystroke dynamics datasets is significantly varied as per the literature review. The selection of consistent and appropriate method is an important issue always demanded in keystroke dynamics domain in order to the performance of one method jumps from 65% to 90%. In our study, two popular machine learning methods: Support Vector Machine with RBF and Fuzzy Rough Nearest Neighbor with VQRS were used in identifying different soft biometric traits and it has been observed that FRNN-VQRS is proved to be the suitable machine learning method that can be adopted in identifying traits in keystroke dynamics domain. The performance of FRNN-VQRS is very impressive, consistent, and significantly better than the previously used leading machine learning method. In this study, we compared our approach with SVM-RBF. Identifying soft biometric traits in keystroke dynamics domain and obtained results are summarized in Table 2. It is clear from the table is that Emotional state, gender, handedness, and a number of hands used can be identified by the analysis of typing pattern.

Table 2. Obtained results in identifying soft biometric traits in keystroke dynamics

| Study | Traits | Factors | Results |
|---|---|---|---|
| [10] | Emotional states | Anger and Excitation | 84% accuracy |
| [4] | Gender | Male and Female | 91% accuracy |
| [8] | Gender | Male and Female | 65%-90% accuracy |
| [8] | Hand(s) used | One hand and Two hands | 90% accuracy |
| [8] | Age group | <30 and ≥30<br><32 and ≥32 | 65%-82% accuracy |
| [8] | Handedness | Left-handed and Right handed | 70%-90% accuracy |
| [9] | Age group | ≤18 and 18+ | <10% EER |
| [14] | Age group | ≤18 and 18+ | 92% accuracy in desktop environment and 84.22% in android environment |

The main objective of this study is two-fold, first to develop a predicting model to identify the proper gender, age group, handedness, hand(s) used, and typing skill of users by analyzing the typing pattern on a conventional keyboard and identify the gender and age group through touchscreen phone for a predefined text, and the second objective is the incorporation of soft biometric information as extra features in keystroke dynamics user recognition system in order to improve the performance in accuracy and time efficiency of the system.

Our objective and contribution of this paper are listed below:

- This study provides an effective and efficient approach to identifying soft biometric information by analyzing the typing pattern on a computer keyboard and a touchscreen phone. The performance of our approach is promising than other approaches in the literature.
- Evaluate and compare our model in identifying traits using multiple, public and authentic keystroke dynamics datasets collected in the different experimental setup in different environments.
- Design, evaluate and compare 9 leading anomaly detectors[22] by combining soft biometric traits with primary keystroke dynamics pattern in user recognition through typing pattern.

Some of few datasets have been used in our experiment in identifying soft biometric traits and to validate the model. But the anomaly detector algorithms have been applied to the dataset collected by Killourhy et. al. [23].

## II. SHARED KEYSTROKE DYNAMICS DATASETS

In keystroke dynamics research, researchers spend more time in the data acquisition section rather than addressing challenging issues because this is the most fundamental and essential section of any behavioral biometric system. As a result, various datasets have been produced but none of this is considered to be a balanced one due to many factors ignored during the creation of dataset. Separate datasets have been created with different experimental setups in 37 years of on-going research and different evaluation criteria have been controlled on each. Researchers have developed datasets considering only their temporal requirement and method of application, this type of datasets are not so neither potential nor balanced. We need very versatile well balanced, reasonable large, containing many variations a data set to make the study fruitful. It is only because of the lack of standards for data collection and benchmarking. Therefore, it has not been possible to make a sound comparison of the different evaluation process. In this paper, we introduced about 11 public authentic datasets on keystroke dynamics that may allow the researchers to make a better benchmarking on keystroke dynamics and to focus on more challenging issues instead of spending time in data acquisition. The keystroke dynamics dataset can be a form of static or dynamic. In this paper, we summarized the static keystroke dynamics datasets.

Loy et. al. [24] in 2005, they have collected the data for a predefined text "try4-mbs", they have used a special pressure sensitive keyboard to collect the data from 100 users 10 times from each user. Total of 1000 samples has been produced. They captured only latency time of the sequences of entered characters and pressure on key. Killourhy et. al. [23] created a dataset from 51 individuals with 50 repetitions in 8 sessions, they captured the keystroke dynamics features Key Duration (KD), Down Down (DD) key latency (DD) and Up Down key latency (UD) for a logically complex typed predefined text ".tie5Roanl". They used a QWERTY keyboard as a sensing device. Bello et al. [25] collected the dataset from 58 users in one session for 15 Spanish sentences and 15 Unix commands. They only captured the time interval between one key press and the next key release in an uncontrolled environment. Giot et al. [26] collected the dataset from 118 users for login information and password in 3 sessions. The sequences of key up and down latencies were captured in this dataset. Giot et. al. [4] in 2012, they produced the datasets from 133 users for 4 repetitions in 12 sessions for a simple predefined text "greyc laboratory". They have used AZERTY keyboard as a sensing device. Captured features are Down Down (DD) key latency, Up Up (UU) key latency, Up Down (UD) key latency and Down Up (DU) key latency. Roth et. al. [27] collected the dataset for the paragraph started by the sentence : "A Tale of Two Cities" written by Charles Dickens, and half page email from 50 users with 4 repetitions in 2 sessions. They have used QWERTY keyboard to captured keystroke sound and di-graph time. Syed-Idrus et al. [28] collected the dataset from 110 users for the five predefined texts. They have used AZERTY and QWERTY keyboards. El-Abed et. al.[9] collected the data from 51 users for the predefined text "rhu.university" by using an android smartphone Nokia Lumia 920. The latency time of the sequences of key press and release have been captured in their dataset.

Table 3. Details of static and shared datasets used in this study to predict traits

| Given Name | Study | Text type | Traits |
|---|---|---|---|
| Dataset A | [23] | ".tie5Roanl" | Gender, age group (<30/30+), handedness, and skill |
| Dataset B | [23] | "4121937162" | Do |
| Dataset C | [23] | "hester" | Do |
| Dataset D | [8] | "leonardo discaprio" | Gender, age group (<30/≥30), handedness, and hand(s) used |
| Dataset E | [8] | "the rolling stons" | Do |
| Dataset F | [8] | "Michael schumaclur" | Do |
| Dataset G | [8] | "red hot chilli perpers" | Do |
| Dataset H | [8] | "united states of america" | Do |
| Dataset I | [29] | "rhu.university" | Gender, and age group (<18/19+) |
| Dataset J | [9] | ".tie5Roanl" | Age group (≤18/18+) |
| Dataset K | [9] | "Mercan Otu" | Do |
| Dataset L | [9] | ".tie5RoanlMercan Otu" | Do |

Antal et.al. [30] collected the dataset from 54 users minimum of 30 repetitions in 2 sessions for three type of texts ".tie5Roanl", "kicsikutyatarka", and "Kktsf2!2014". They used the Nexus 7 tablet and Mobil LG Optimus L7 II P710 as a sensing device. Key pressure, acceleration, and velocity along with timing features were captured and produced. Jugurta et. al. [31] collected the data from 8 to 15 number of users to captured Down Down (DD) key latency for the predefined simple daily used texts "chocolate", "zebra", "banana", "taxi", "computador calcula" by using standard 101/102 keys, Brazilian layout - similar to the EUA layout. Uzun et. al. [9] collected the data from 100 users to capture key duration and Down Down (DD) and Up Down (UD) key latency for two type of texts. One is simple ("Mercan Otu") and another is a strong password typed (".tie5Roanl") to identify the child user from an adult. They have used a QWERTY keyboard as a sensing device.

Some of the few datasets we have used in our experiment. Datasets with soft biometric information were selected to be used in our experiment. The datasets created by Killourhy et al. [32], Idrus et. al. [33], Yuzun et al. [9] and El-Abed et al. [29] were used in our experiment. The names of each dataset have been assigned to identify all the datasets throughout this paper described in Table 3.

Sample distribution of different classes. As we see in our experiment, the performance of SVM is promising only when the dataset is equally distributed among the classes.

## III. METHODOLOGY

The following series of steps were used in our experiment. First, we have collected the publicly available authentic and recognize datasets for a different type of text in different environments. Then we recalculated the four timing features by the following equations due to the unavailability of all features in all the datasets:

The timing features of the typing pattern are as follows:

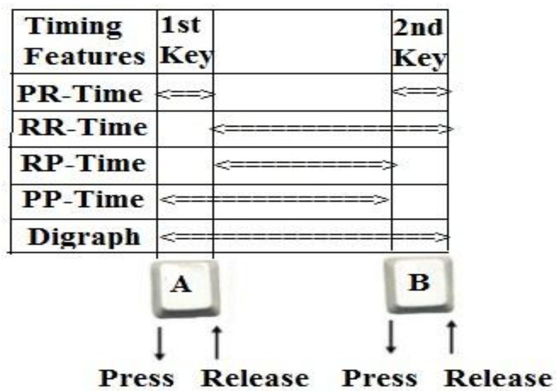


Figure. 1. Timing features of keystroke dynamic characteristics

We normalized the datasets within the range in between -1 to 1 to speed up the computing process.

Two leading machine learning methods were used to develop the model: SVM and FRNN. Fuzzy-rough nearest neighbor with a vaguely quantified rough set (FRNN-VQRS) [34] classification algorithm is an alternative to Sarkar's fuzzy-rough ownership function (FRNN-O) approach [35]. In SVM, we have used RBF with the cost function (C=128, $\gamma$=0.125) as per the guided by [36]. In FRNN, we have used VQRS with tuning the parameter, a number of the nearest neighbor, k=6.

To get the impact of soft biometric traits, each sample is manually labeled with the score 0 and 1 for the real different gender, age group, handedness and typing skill of the user. The next stage, we have re-implemented 9 anomaly detectors methods and evaluated the performance of each dataset with the combination of soft biometric information. The similar procedure was used to train and test the samples. Same evaluation methodology was followed as per the study [23] described except median proximity instead of mean suggested to create the template of the user-guided by the study [37]. The Equal Error Rates (EERs) were recorded for each user. The average EER is a parameter to evaluate the performance of all anomaly detectors. EER is the value where FAR and FRR both are same.

## IV. OBTAINED RESULTS

In this part, the obtained results from the evaluation process have been presented. Two leading machine learning methods were applied to 12 shared datasets. Here, each dataset is different from others on the basis of data acquisition methodology, text selection, number of samples, categorization of classes, and the use of sensing devices. The accuracy in identifying traits with 10 fold cross-validation test-option was recorded and presented in Figure 2. The figure not only indicates the performance of FRNN and SVM in identifying multiple soft biometric traits, but it also compares the performance of each dataset.

The obtained results indicate that the gender can be predicted with the accuracy of 83% to 95% by using FRNN. This result is significantly different from the previously used SVM by the study [8]. Recognizing gender is an important soft biometric trait is not only used to improve the accuracy of user recognition system also could help to the social network site for face free and loyal user base.

Identifying the age group is an important issue in keystroke dynamics domain. The 75% to 95% accuracy was recorded in identifying the age group (<30/30+) by our approach. Identifying the age group (<18/18+) also was recorded to separate the child users from adult users based on their typing rhythm. So, we can protect the teens from the looming threads on the Internet or we can filter the content which is more appropriate for that category of users by implementing the autosensing firewall appropriate for the users.

Handedness of the user can be predicted as per the results. The 94% to 99% accuracy can be achieved by identifying the handedness of the users by their typing style.

The 89% to 95% accuracy was recorded in identifying the typing skill on various shared datasets. It can be used as soft biometric traits to improve the accuracy of user recognition through keystroke dynamics characteristics.

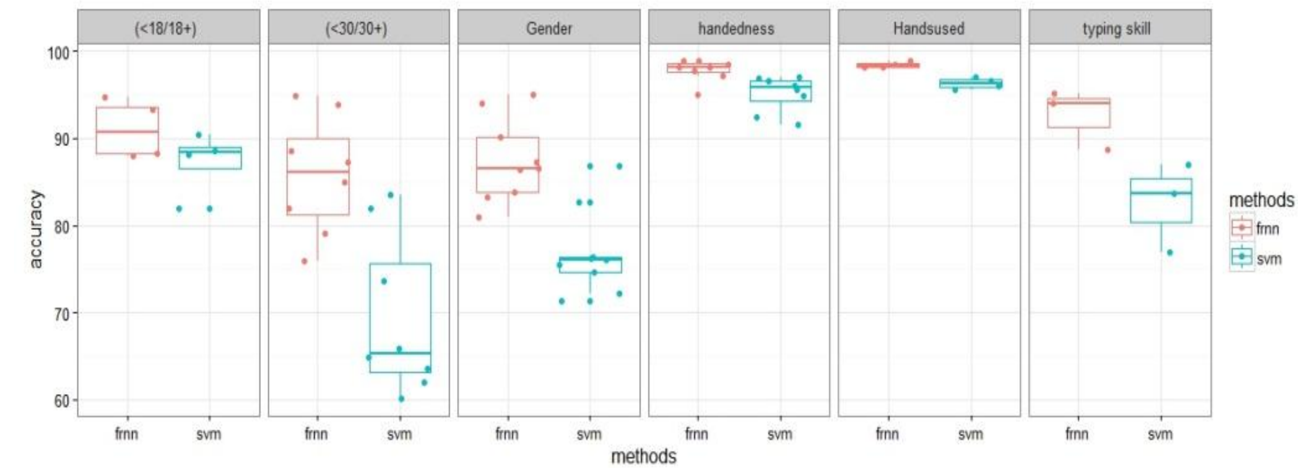


Figure. 2. Comparison chart of two methods for identifying traits

The results recorded in identifying traits are promising and significantly better than the previously used SVM in all cases.

Figure 3 represents the evaluation performance of 9 anomaly detectors described in the study [39], EERs in % on three datasets Dataset A, Dataset B, and Dataset C were presented. The EER jumps from 10.69% to 2.53% by incorporating gender age handedness, and typing skill mentioned for Dataset A in Lorentzian anomaly detection. Results for Dataset B jumps from 11.2% to 2.73, where 12.69% to 4.41 for Dataset C. The improvement of EER does not depend on the text pattern as per the results recorded for Dataset B and Dataset C. The performance of detectors in each dataset was presented. It is established from the figure that instead of only using gender as an extra feature, the use of multiple soft biometric traits is significantly better to improve the performance of the detectors.

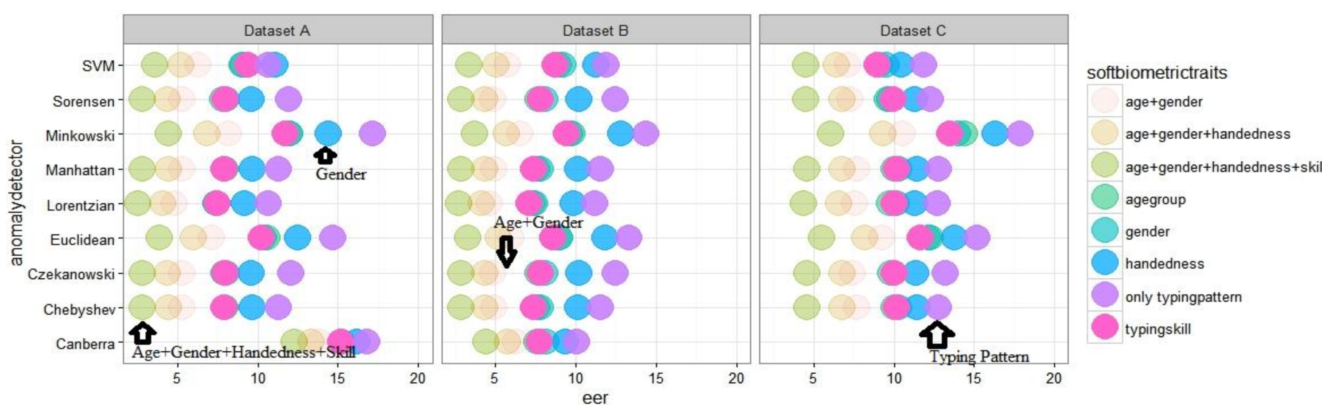


Figure. 3. Comparing anomaly detectors with the incorporation of soft biometric traits

## V. CONCLUSION AND FUTURE SCOPE

The performance of SVM is promising on fully balanced datasets where the samples of the different classes are equally distributed. But it may happen; datasets may not be balanced all the time. In this situation, the use of FRNN is effective as we see in our experimental results which is an efficient model in identifying the gender, age group, handedness, hand(s) used, and typing skill by analyzing the typing pattern. The model is validated on various shared datasets collected in different environments. The obtained results are promising as it is evident from our experiment. We also compared our model with previously used leading machine learning method. In this paper, 11 public authentic datasets on keystroke dynamics and distribution of the collected samples are analyzed that may allow the researchers to make a better benchmarking on keystroke dynamics and to focus on more challenging issues instead of spending time in data acquisition. Keystroke dynamics characteristics promise a parameter which can be easily captured and available in web-based applications. The paper explained the activities on a computer keyboard and touchscreen are behavioral biometric characteristics can be used to predict some of the soft biometric characteristics to deal with the problem of fake accounts and would enable to create a more loyal and authentic social networking site. But in this paper, soft biometrics was used to address the problems associated with keystroke dynamics biometrics.

Two machine learning methods were used in our experiment and compared their performance. Our proposed approach FRNN-VQRS, a new approach to FRNN is significantly better than previously used SVM with RBF to determine the personality traits in desktop and Android environments. The performance of SVM will be comparable with the FRNN if the samples in different classes are equally distributed. But the evaluation performance of FRNN-VQRS is consistent in all cases in our study. The effective method has been applied to compare the evaluation performance of used two machine learning models. Nowadays, smartphone with added sensors gives an extra feature to build this model which will be more appropriate.

## REFERENCES


[1] D. Bartmann, I. Bakdi, and M. Achatz, “On the Design of an Authentication System Based on Keystroke Dynamics Using a Predefined Input Text,” *Int. J. Inf. Secur. Priv.*, vol. 1, no. 2, pp. 1–12, 2007.

[2] P. H. Pisani, R. Giot, A. C. P. L. F. De Carvalho, and A. C. Lorena, “Enhanced template update: Application to keystroke dynamics,” *Comput. Secur.*, vol. 60, pp. 134–153, 2016.

[3] P. S. Teh, S. Yue, and A. B. Teoh, “Feature Fusion Approach on Keystroke Dynamics Efficiency Enhancement,” *Int. J. Cyber-Security Digit. Forensics*, vol. 1, no. 1, pp. 20–31, 2012.

[4] R. Giot and C. Rosenberger, “A new soft biometric approach for keystroke dynamics based on gender recognition,” *Int. J. Inf. Technol. Manag. Spec. Issue Adv. Trends Biometrics*, vol. 11, no. August, pp. 1–16, 2012.

[5] A. K. Jain, S. C. Dass, and K. Nandakumar, “Can soft biometric traits assist user recognition ?,” pp. 1–12.

[6] A. Dantcheva, C. Velardo, A. D’Angelo, and J.-L. Dugelay, “Bag of soft biometrics for person identification: New trends and challenges,” *Multimed. Tools Appl.*, vol. 51, no. 2, pp. 739–777, 2011.

[7] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, “Integrating Faces , Fingerprints , and Soft Biometric Traits for User Recognition,” no. May, pp. 259–269, 2004.

[8] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, “Soft Biometrics For Keystroke Dynamics,” in *10th International Conference on Image Analysis and Recognition (ICIAR)*, 2013, pp. 11–18.

[9] Y. Uzun, K. Bicakci, and Y. Uzunay, “Could We Distinguish Child Users from Adults Using Keystroke Dynamics?,” 2014.

[10] C. Epp, M. Lippold, and R. L. Mandryk, “Identifying Emotional States Using Keystroke Dynamics,” *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, pp. 715–724, 2011.

[11] P. R. Letters *et al.*, “Soft biometrics — combining body weight and fat measurements with fingerprint biometrics,” no. May 2016, 2006.

[12] A. K. Jain and U. Park, “Facial marks: Soft biometric for face recognition,” *Proc. - Int. Conf. Image Process. ICIP*, pp. 37–40, 2009.

[13] Z. Li, X. Zhou, and T. S. Huang, “Spatial Gaussian mixture model for gender recognition,” in *IEEE 16th International Conference on Image Processing (ICIP 2009)*, 2009.

[14] S. Roy, U. Roy, and D. D. Sinha, “ACO-Random Forest Approach to Protect the Kids from Internet Threats through Keystroke,” *Int. J. Eng. Technol.*, vol. (Accepted), pp. 2–9, 2017.

[15] J. L. Wayman, “Large-scale Civilian Biometric Systems-Issues and Feasibility,” in *Proceedings of Card Tech/Secur Tech ID*, 1997.

[16] S. Gutta, J. R. J. Huang, P. Jonathon, and H. Wechsler, “Mixture of experts for classification of gender, ethnic origin, and pose of human faces,” *IEEE Trans. Neural Networks*, vol. 11, no. 4, pp. 948–960, 2000.

[17] A. K. Jain, S. C. Dass, and K. Nandakumar, “Soft Biometric Traits for Personal Recognition Systems,” *Proc. Int. Conf. Biometric Authentication*, no. July, pp. 731–738, 2004.

[18] X. Lu and A. Jain, “Ethnicity identification from face images,” *Proc. SPIE Conf. Biometric Technol. Hum. Identification*, vol. 5404, pp. 114–123, 2004.

[19] H. Ailisto, E. Vildjiounaite, M. Lindholm, S. M. Mäkelä, and J. Peltola, “Soft biometrics-combining body weight and fat measurements with fingerprint biometrics,” *Pattern Recognit. Lett.*, vol. 27, no. 5, pp. 325–334, 2006.

[20] U. Park and A. Jain, “Face matching and retrival using soft biometrics Information Forensics and Security,” *IEEE Trans.*, vol. 5, no. 3, pp. 406–415, 2010.


 

[21] S. Roy, U. Roy, and D. D. Sinha, *Efficacy of Typing Pattern Analysis in Identifying Soft Biometric Information and Its Impact in User Recognition*, vol. 10590 LNCS. 2017.
[22] S. Roy, U. Roy, and D. D. Sinha, "Comparative study of various features-mining-based classifiers in different keystroke dynamics datasets," in *Smart Innovation, Systems and Technologies*, vol. 50, 2016.
[23] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *Proceedings of the International Conference on Dependable Systems and Networks*, 2009, pp. 125–134.
[24] C. C. Loy, C. P. Lim, and W. K. Lai, "Pressure-based typing biometrics user authentication using the fuzzy ARTMAP neural network," in *International Conference on Neural Information Processing (ICONIP)*, 2005.
[25] L. Bello and M. Bertacchini, "Collection and publication of a fixed text keystroke dynamics dataset," *CACIC 2010 - XVI Congr. ARGENTINO CIENCIAS LA Comput.*, pp. 822–831, 2010.
[26] R. Giot, M. El-Abed, and C. Rosenberger, "Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis," *Intell. Inf. hiding andmultimedia signal Process.*, pp. 11–15, 2012.
[27] J. Roth, X. Liu, A. Ross, and D. Metaxas, "Biometric Authentication via Keystroke Sound," *2013 Int. Conf. biometrics*, pp. 1–8, 2013.
[28] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*, 2013, no. September, pp. 1–8.
[29] M. El-Abed, M. Dafer, and R. El Khayat, "RHU Keystroke: A mobile-based benchmark for keystroke dynamics systems," *2014 Int. Carnahan Conf. Secur. Technol.*, pp. 1–4, 2014.
[30] M. Antal and L. Z. Szabo, "An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices," *Proc. - 2015 20th Int. Conf. Control Syst. Comput. Sci. CSCS 2015*, pp. 343–350, 2015.
[31] J. Montalvão, E. O. Freire, M. A. Bezerra, and R. Garcia, "Contributions to empirical analysis of keystroke dynamics in passwords," *Pattern Recognit. Lett.*, 2015.
[32] K. S. Killourhy, "A Scientific Understanding of Keystroke Dynamics," *Dr. Thesis, Sch. Comput. Sci. Comput. Sci. Dep. CarnegieMellon Univ. Pittsburgh, PA 15213*, no. January, pp. 1–198, 2012.
[33] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," *Biometrics Spec. Interes. Gr. (BIOSIG), 2013 Int. Conf.*, no. September, pp. 1–8, 2013.
[34] R. Jensen and C. Cornelis, "Fuzzy Rough Nearest Neighbour Classification and Prediction," *Theor. Comput. Sci.*, vol. 412(42), pp. 5871–5884, 2011.
[35] M. Sarkar, "Fuzzy-rough nearest neighbor algorithms in classification," *Fuzzy Sets Syst.*, vol. 158, no. 19, pp. 2134–2152, 2007.
[36] C.-W. Hsu, C.-C. Chang, and C.-J. Lin, "A Practical Guide to Support Vector Classification," *BJU Int.*, vol. 101, no. 1, pp. 1396–400, 2008.
[37] S. J. Alghamdi and L. A. Elrefaei, "Dynamic User Verification Using Touch Keystroke Based on Medians Vector Proximity," *Proc. - 7th Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSyN 2015*, pp. 121–126, 2015.
[38] S. Zulkarnain *et al.*, "Keystroke Dynamics Performance Enhancement With Soft Biometrics."
[39] S. Roy, U. Roy, and D. D. Sinha, "Comparative Study of Various Features-Mining-Based Classifiers in Different Keystroke Dynamics Datasets," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems*, 2016, vol. 2, pp. 155–164.


## AUTHORS PROFILE

Soumen Roy is with University of Calcutta since last 4 years as a research scholar. He is also working with Bagnan College, Bagnan, Howrah, India for last 8 years as a teacher. He has also one year of experience in software development. He has published more than 20 international paper in the form of journal and conference proceeding.

After the completion of his Ph.D. from Department of Mathematics Visva-Bharati he went to the LAVAL University, Quebec, Canada for the Post Doctoral work in 1994. He worked at Indian Association for the Cultivation of Science, Jadavpur, Kolkata 32 as CSIR Scientist Pool during 1996-1997. He Joint the Visva-Bharati at the end of 1997 as Asst. Prof in Computer Science to teach the MCA course. He worked as Visiting Scientist in Academia Sinica, Taipei Taiwan during 2001 and 2002. He worked as Professor in IT in Assam University Silchar, Assam during 2008-2009. Presently he is a Professor and Former Head of the Department, Department of Computer & System Sciences, Visva-Bharati. He has been guiding Ph.D. students since long time and many students have been awarded Ph.D. under his supervision.

Devadatta Sinha has more than thirty eight of experience in the field of Computer Science and Engineering in research and teaching. He worked as Faculty member in BIT Mesra, Ranchi, Jadavpur University, University of Calcutta. He written a number of research papers in National and International Journals, Conference Proceedings. He also written a number of expository articles in periodicals, books, monographs. He has research interests include Software Engineering, Parallel and Distributed Algorithms, Bioinformatics, Computational Intelligence, Computer Education, Mathematical Ecology, Networking. He guided research students for Ph.D, in Computer Science and Engineering and M.Tech, B.Tech and M.Sc students for their dissertation. He performed as Sectional President, Section of Computer Science, Indian Science Congress Association (1994). He is a Fellow in Computer Society of India.

 