Biometric Authentication and Identification using Behavioral Biometrics Technique of Signature Verification

Shalini Dhiman, Munish Sabharwal

Abstract*: Authentication using biometrics is on the rise due to various security concerns and especially in India with the advent of Digital India concept promoting the wide use of aadhar as an authentication mechanism. The authentication using a login and a password are fading away due to the various malpractices and fraudulent methods that have been developed which pose a threat to this kind of authentication and security mechanism. Signature verification is one of the important aspects of biometric authentication which is slowly finding its use in certain niche organizations. The present study uses an ensemble approach, stacking to authenticate or validate a user by his signature and proposes a hybrid model using three algorithms namely, Random Tree, Logistic Regression & Multi-Layer Perceptron for achieving better accuracy.

***Index Terms*: Signature verification, Behavioral biometrics, Authentication, Random Tree, Logistic Regression, MLP.**

I. INTRODUCTION

There have been a lot of developments in authentication solutions for a secure transaction along with the growing popularity of digitization. Munish Sabharwal et al. [1] has presented the ideology of *DIGITAL INDIA* in his paper describing the various comprehensive application of aadhar for an extensive socio-economic impact on Indian society**.** As the knowledge-based tokens/data can be forgotten or stolen, so they can no longer be used further whereas biometric-based tokens provide a great solution to this problem with great ease and high level of the secure environment [2].

Biometrics refers to the main solution for authentication of a user with the help of his traits and characteristics. Traits used are nothing but unique attributes which describes user that helps in identification, physiological attributes remain static all along whereas behavioral attributes are dynamic attributes. Some dynamic attributes like signatures are widely used for identification [3, 4]. There is a need for biometric authentication because the concept of digitization has made users more vulnerable to threats of identity theft. The current scenario of identifying a user is through a username and a password. Keeping in mind the remembrance power of a user, he tends to use the same password in various other applications and platforms which increases his exposure to many malicious elements present outside seeking an opportunity to steal any valuable information. Thus, in order to confirm user identity, an additional layer of security is a must. The concept of biometric authentication is introduced to overcome this situation [5, 6].

Munish Sabharwal et al. [7] discussed various types of biometrics discovered so far. He has summarized all the types as well as the technologies used in each type for authentication. Therefore, biometrics can be categorized into three types: Physiological, Behavioral and Hybrid. Physiological Biometrics deals with the analysis of human physiological patterns. It lays emphasis on the outcome as physiological characteristics are static in nature like Thumb, Fingerprint, Palm**,** Face, Iris, Retina, Lip, Ear, etc. They have great use in institutions and various organizations. They can guarantee a person originality [8]. Behavioral biometrics deals with the analysis of a human behavioral pattern used to further authenticate a user. It lays emphasis on the way it conducts rather than the outcome. For example, it doesn't care whether the user enters a correct password or not, but how a user enters it. It analyses his typing speed which is further categorized in Keystroke biometrics [9]. It can be easily obtained from a reliable source without any chance of misconduct. That is the main reason for their rise. They can be proved to be useful in a situation where the data is not easily obtained and cannot guarantee its originality [10]. Hybrid biometrics deals with the combinational impact of both the biometrics, using human physiological patterns along with behavioral pattern [7].

Signature Verification biometrics gaining wide acceptance as biometrics for user authentication. The dataset can be easily obtained from a user. A training and test signature dataset are created. The training dataset is used to train the machine whereas test dataset is used to test whether it matches or not. A comparison is made and a matching score is generated. A decision is made based on matching score whether to claim the signature as real or fake [11]. There are mainly two forms available to date: Offline and Online Signature Verification.

Revised Manuscript Received on July 10, 2019.

Shalini Dhiman, CSE Department, Chandigarh University, Chandigarh, India.

Munish Sabharwal, CSE Department, Chandigarh University, Chandigarh, India.

Both have their own significance and can be used accordingly. In offline signature verification, verification is done by matching the samples manually whereas, in online signature verification, verification is done by a machine by considering various other parameters like velocity, pressure, trajectory, and various other scientific terms which makes it almost impossible to forge an identity. Therefore, online verification is preferred over offline [4].

II. LITERATURE REVIEW

Much recent advancement has been done in the area of behavioral biometrics using various techniques.

Munish Sabharwal et. al. [10] surveyed various kinds of biometric technologies updated until now. He has also suggested a multi-modal biometric authentication and secure transaction operation framework for e-banking and the same concept has been discussed by him in [11] along with various authentication technologies in e-banking.

Renu Bhatia et al. (2013) explores various aspects of biometrics and its types like physiological and behavioral biometrics. She further elaborates its features and also discusses some examples related to it like iris and retina scan [15].

Ioannis Rigas et al. (2012) [35] This paper further explores the area of biometric identification and gives human eye movement as a new trait for identification. It takes into account the movement of the eye on a computer screen and uses it for distinguishing users.

Many reviews have been presented by many researchers like Shalini Dhiman et. al. [12] presented a review of various types of methods used for verification of signatures whether online or offline. Various kinds of biometrics are also discussed. It provides a wide range of information regarding the biometric system and security.

Anil K. Jain et al. (2004) [17] In his paper, he talks about the basic concept of biometrics and the recognition based on it, its positive and negative aspects. It gives us insight about authorization and authenticity concepts.

[18] It shed light on the working of behavioral biometrics with real-world applications. It also discusses the benefits and utility of biometrics technology. Privacy concerns and accuracy/performance considerations are also addressed.

Sukhdeep Singh et al. (2013) [33] It further addresses the concept of ear recognition in the field of physiological biometrics. It can be considered as a good approach to verify a person.

Farhana Javed Zareen et al. (2014) presents a detailed review and compares various methods of biometric signature verification, online as well as offline [16].

Jonas Richiardi et al. (2003) [2] discusses the use of Gaussian Mixture Models for verification of online signatures. Since it is online, it considers various complicated parameters like trajectory, projection, angles of a signature. It uses 50 user subset of MCYT multimodal dataset.

Roman V. Yampolskiy et al. (2009) [19] It uses the concept of biometrics with the gaming network for behavioral intrusion detection approach. The approach is used to extract a player's profile in the game of poker. It works on detecting any security breach in the game server.

Rohan V. Ponkshe et al. (2015) [3] discusses concerns of network security and mouse movements and keystroke dynamics as a solution. Similarly, security concerns have been discussed by Robert Moskovitch [4]. The technique of keystroke dynamics is explored and how it can be used to minimize the aftermath of identity theft and how to prevent it. It works on augmenting the login process and proposed behavioral biometrics as a solution. Umut Uludag et al. (2004) [5] In this paper, the concept of user authentication using cryptosystems is given. This paper presents various methods of binding biometrics with cryptographic key i.e. key contents cannot be revealed without proper biometric authentication. Sheela Shankar et al. (2016) [6] This paper works toward the robustness of the verification system. It surveys biometric techniques and its usage. It shed some light on technical and security-related issues of the biometric system.

Nilson Donizete Guerin Jr. et al. (2015) [7] works on proposing an online verification system. A system that will verify signatures and cursive words by using certain parameters like a histogram of angles, velocity and Fourier descriptors. It will be applicable to mobile phones to unlock various applications like viewing the gallery, unlocking messaging app, camera, etc. Similarly, many mobile-based authentications are carried out by Frank Zoebisch to propose a method for building a tool for verification of signatures. The tool will support the forgery test on mobile phones [8].

N.L. Clarke et al. [9] lay emphasis on the need of using biometric authentication for mobile phones as phones usually use weak authentication methods like PIN and passwords which can result in high chances of hacking. This paper names keystroke dynamics as a better biometric approach.

Luiz G. Hafemann et al. (2016) [26] This paper proposes formulations of feature learning for Offline Signature Verification. A novel method is proposed which uses knowledge of forgeries. These learned features are further used to train various classifiers. In his next paper, he has further enhanced his previous research by providing ways to reduce Error rate using multiple classifiers. He has also presented a visual analysis of the feature space learned by the model in [27].

Similarly, Luiz G. Hafemann et al. (2017) [13] gives us the analyses done in the arena of signature verification both online and offline. Various techniques are also explored which are needed to verify user identity. Recent advancements are also discussed focusing on Deep Learning Methods for feature extraction. Mandeep Kaur et al. (2016) works on improving the efficiency of the Signature Verification system. It also explores various verification techniques used to distinguish real and forged signatures. It follows an approach of the calculating distance between the input signature and threshold [14].

A. Namboodiri et al. (2006) [28] This paper tries to verify writer identification not only using text but also multiple languages and scripts. It uses both online as well as offline handwritten data. It often requires a large amount of data for better results.

Y. Liu et al. (2015) [29] This paper tries to approach the problem of online signature verification using a discrete cosine transform (DCT) and sparse representation. Andreas Fischer et al. (2015) [30] In this paper, score normalization is proposed for the problem of lack of dataset in the area of signature verification using DTW. It works on two-stage normalization, one for simple forgery and other for skilled forgery.

Sadhna et al. (2015) [31] This paper explores various features and aspects of behavioral biometrics. This paper proposes a combination of a graphical approach using a multi-structure algorithm and ANN. It performs various other analyses on handwritten signatures.

Ishan Bhardwaj et al. (2016) [32] This paper discusses the concept of keystroke dynamics and how it can be used in the verification system. It also illustrates the approach of fingerprint dynamics. It can also be categorized under pattern recognition.

K. Cpałka et al. (2016) [34] In this paper, the signature partitioning approach is proposed for verification purpose. Effective methods for verification of signatures are discussed.

Abhishek Sharma et al. (2017) [20] discusses the technique of DTW cost matrix for verification of online signature verification. A slightly different approach than the traditional method is followed whereas using the same approach, a set of features are derived from the Gaussian Mixture Model framework in [21].

[22] It depicts the summary, usage, syntax, code samples, environments and licensing information of Random tree classifier used in machine learning.

Ranjan Kumar Singh et al. (2017) [23] This paper tries to perform offline signature verification using decision tree classifiers such as J48 and Random Forest considering various features extraction and image processing techniques.

[24] It gives us information about logistic regression and logistic function like what it actually is, how does it work, what are the concepts behind it and other main concepts like dataset preparation and making a prediction using logistic regression in machine learning.

[25] It shed some light on the concept of the confusion matrix and its related terms.

The studies by Munish, first [36], facilitated the researcher in the overall preparation of literature review and planning for the overall research and the second [37], assisted in analysis. After exhaustive research in the field of biometric authentication, Signature verification emerges out to be an upcoming biometric authentication technique. It was found that many researchers have contributed in this field but few have laid emphasis on Signature verification using a hybrid model of Random Tree, Logistic Regression & Multi-Layer Perceptron, these areas are explored in this study.

III. METHODOLOGY

As per the methodology of the paper illustrated in figure1, following methods are discussed below.

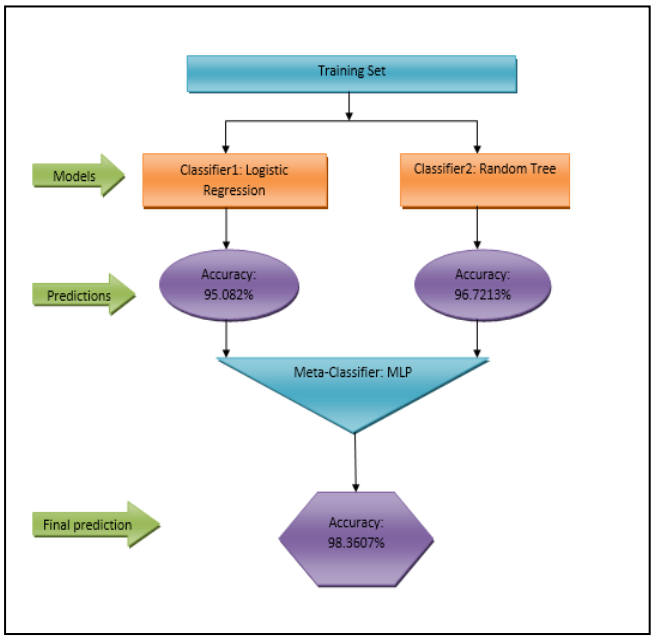

Fig. 1. Research Methodology

A. *Dataset* Acquisition

Dataset is prepared from a reliable source according to the offline and online form. It mainly involves the comparison of the new sample to the old one. It is mainly carried out for the verification and identification of a user's identity. A self-created dataset of 61 images of signature of users at various angles for training and testing purpose. This is primary dataset created only for this purpose. The dataset contains 45 real and 16 forged signatures. A .arff file is created for the implementation which lists dataset elements as per its syntax. This file is further used in WEKA tool.

B. Feature Extraction

Feature extraction can be seen as a pivotal aspect in a signature verification system whether it is online or offline. It considers local as well as global features of a signature. Local features are function based, considered at each point of the signature's trajectory and have a low error rate whereas global features are considered as a whole and have a high error rate and the low computational load [4].

Image package filter for extracting features and ColorLayout & EdgeHistogram Filter for further extraction of our signatures are used which shows results in figure2.

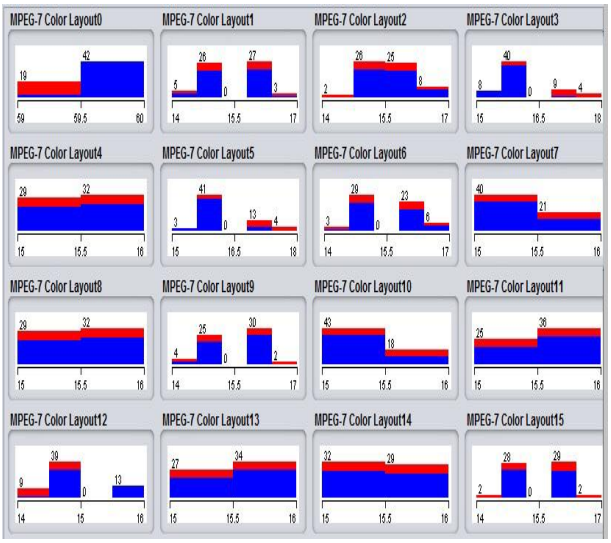

Fig. 2. Extracted features

C. Approaches

There are mainly two approaches followed for signature verification: writer dependent and writer independent. In the first case, the writer is dependent on the machine for verification, i.e., the machine is trained for each user by using his real signatures, whereas, in the second case, the writer is independent of the machine i.e., the machine is trained to compare a query signature with a reference one[12].

D. Ensemble Method- Stacking

Stacking is nothing but using two or more classifiers for improving accuracy and reducing error rates. It consists of one meta-classifier and rests are simple classifiers. Meta classifier results in the final classification.

Implementation of our experiment is carried out in Data Mining Tool, WEKA. Multi-Layer Perceptron classifier is used as meta-classifier and two algorithms, Random Tree and Logistic Regression are used as simple classifiers.

IV. EXPERIMENTAL RESULTS

In our experiment, mainly three classifiers are used. The first attempt uses Logistic Regression as classifier, the second attempt uses Random Tree as classifier and the final attempt uses Stacking algorithm and uses three classifiers, out of which one is meta-classifier (MLP) and the other two (classifier1: Logistic Regression, classifier2: Random Tree) are simple classifiers used only for increasing accuracy. The ensemble approach is followed. In WEKA tool, stacking algorithm follows ensemble approach. The classifiers used are explained with the results below and the outcome of the implementation by applying random tree is shown in figure3, logistic regression in figure4 and stacking which uses MLP as meta-classifier in figure5.

A. Classifier1: Logistic Regression

Another classifier used for verification of signatures is Logistic Regression. It uses the sigmoid function in an s-shaped graph to make the probability [15]. It deals with binary values (0 or 1) or values can vary between 0 and 1.

```
Time taken to build model: 0.01 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances          58               95.082  %
Incorrectly Classified Instances         3                4.918  %
Kappa statistic                          0.8802
Mean absolute error                      0.0492
Root mean squared error                  0.2218
Relative absolute error                 12.5385 %
Root relative squared error             50.2294 %
Total Number of Instances               61
```

Fig. 3. Logistic regression (*Classifier1*)

B. Classifier2: Random Tree

Random Tree is an unsupervised machine learning algorithm also known as decision tree algorithm which is mainly used for classification purpose[13, 14]. It is best known for providing better accuracy in terms of image classification problems and also works on segmented images.

```
Time taken to build model: 0 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances          59               96.7213 %
Incorrectly Classified Instances         2                3.2787 %
Kappa statistic                          0.9117
Mean absolute error                      0.0328
Root mean squared error                  0.1811
Relative absolute error                  8.359  %
Root relative squared error             41.0121 %
Total Number of Instances               61
```

Fig. 4. Random Tree results (*Classifier2*)

C. Meta-Classifier: Multi-Layer Perceptron

MLP comes under the area of neural network and deep Learning. It is one of the main model technique usedfor training the machine for verification and identification purpose. CNN is used to train the machine for learning features of the signature dataset(pixels, as in images). They are considered for both systems i.e. writer dependent and writer in dependent systems.

For better accuracy and results, multiple networks are trained on the features extracted, while other networks are used to form a decision based on the output obtained[12]. Recently, CNN has been used in the area of verification and identification using images.

```
Time taken to build model: 0.14 seconds

=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances          60               98.3607 %
Incorrectly Classified Instances         1                1.6393 %
Kappa statistic                          0.9568
Mean absolute error                      0.0255
Root mean squared error                  0.125
Relative absolute error                  6.5125 %
Root relative squared error             28.3149 %
Total Number of Instances               61
```

Fig. 5. MLP results (*Meta-classiifer*)

Confusion Matrix can be defined as a table which is often used to describe the performance of a classification model on a dataset [16]. In our implementation, confusion matrix gives certain value of true positive(TP=45), false positive(FP=0), false negative(FN=1) and true negative(TN=15). It distinguishes the data as real and fake as in figure6.

```
=== Confusion Matrix ===

  a  b   <-- classified as
 45  0 |  a = REAL
  1 15 |  b = FAKE
```

Fig. 6. Confusion matrix

V. RESULTS AND DISCUSSIONS

The ensemble method(Stacking) is used for this classification problem. The algorithms we have used provide much better accuracy and less error rate than other methods. MLP is now widely considered the best choice for extracting features which is why we have used this algorithm as meta-classifier. The result of the experiment is shown in table1.

This type of architecture scale out is better than fully connected models for larger input sizes, which have a less number of training parameters. This is a must property for the problem, though we cannot deduct the signature images much more than allowing risk for loss of details, further which might enable bifurcating between good forgeries and actual signatures [17, 18].

Authors use other metrics to compare - the False Acceptance rates for different types of forgery and the Average Error Rate among all types of error. Although, we have applied stacking algorithm with two classifiers (Random Tree & Logistic Regression) and meta-classifier (MLP) and results came out to be a classifier with good accuracy of 98.3607% and an error rate of 1.6393%.

TABLE I. EXPERIMENTAL RESULTS

MODEL	ACCURACY	ERROR RATE
Logistic Regression	95.082%	4.918%
Random Tree	96.7213%	3.2787%
Hybrid(Meta-classifier: MLP)	98.3607%	1.6393%

VI. CONCLUSION

The study verifies signatures using machine learning algorithms: Logistic Regression, Random Tree and Multi-Layer Perceptron using feature extraction techniques on the dataset. The study shows that signature verification using more than one classifier achieve a far better level of results than using only one classifier. The results show that the study has achieved a good accuracy of 98.3607% by using MLP as meta-classifier.

ACKNOWLEDGMENT

This is to show First author profound gratitude to Dr. Munish Sabharwal, Associate Dean & Professor, Department of Computer Science & Engineering, Chandigarh University, India, for always motivating. First author is sincerely thankful to him for guiding through the entire research work.

REFERENCES

1. Poster presentation “DIGITAL INDIA: The comprehensive application of aadhar for an extensive socio-economic impact on Indian society” in the “India International Science Festival (IISF) - Young Scientists" Conclave (YSC), 2016” organized by Ministry of Science & Technology, Ministry of Earth Sciences, National Physical Laboratory and CSIR on December 8-11, 2016.
2. Jonas Richiardi and Andrzej Drygajlo (2003), Gaussian Mixture Models for Online Signature Verification. ACM 1581137796/03/00011.
3. Rohan V. Ponkshe, Prof. Vikrant Chole (2015), Keystroke and Mouse Dynamics: A Review on Behavioral Biometrics. International Journal of Computer Science and Mobile Computing.
4. Robert Moskovitch, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafić, Ahmet Camtepe, Bernhard Löhlein, Ulrich Heister, Sebastian Möller, Lior Rokach, Yuval Elovici, Identity Theft, Computers, and Behavioral Biometrics.
5. Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K. Jain,”Biometric Cryptosystems: Issues and Challenges” Proceedings of the IEEE . July 2004
6. Sheela Shankar, V.R Udupi, Rahul Dasharath Gavas (2016), “Biometric Verification, Security Concerns and Related Issues - A Comprehensive Study”, I.J. Information Technology and Computer Science, DOI: 10.5815/ijitcs.2016.04.06
7. Nilson Donizete Guerin Jr. (2015), ”Text-dependent User Verification of Handwritten Words and Signatures on Mobile Devices”, The Computer Journal Advance Access, Section C: Computational Intelligence, Machine Learning, and Data Analytics The Computer Journal.

8. Frank Zoebisch, Claus Vielhauer (2003), "A Test Tool to Support Brut-Force Online And Offline Signature Forgery Tests on Mobile Devices", IEEE.
9. N.L. Clarke1, S.M. Furnell1 & P.L. Reynolds (2002)," Biometric Authentication for Mobile Devices", 3rd Australian Information Warfare and Security Conference.
10. Munish Sabharwal, "Multi-Modal Biometric Authentication and Secure Transaction Operation Framework for E-Banking" accepted for publication in International Journal of Business Data Communications and Network (IJBDCN) Vol. 11, Issue 1 pp, to be published.
11. Munish Sabharwal, "The summation of potential biometric types and technologies for authentication in e-banking", International Journal for Scientific Review and Research in Engineering and Technology, ISSN (online): 2455-3603, Vol. 1, Issue 2, pp. 83-92, Feb 2016.
12. Shalini Dhiman, "Behavioural Biometric Authentication and Identification using Signature Verification: A Survey" accepted for publication in the International Conference on Intelligent Machines (ICIM,19), to be published.
13. Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira, " Offline Handwritten Signature Verification - Literature Review" 978-1-5386-1842-4/17/$31.00 c 2017 IEEE (2017).
14. Mandeep Kaur, Sonika jindal, "Survey on Offline Signature Recognition Techniques", International Journal of Engineering Trends and Technology(IJETT)–Vol-36,DOI:10.14445/22315381/IJETT-V36P257. (2016).
15. Renu Bhatia:, "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, ISSN: 2277 128X
16. Farhana Javed Zareen, Suraiya Jabin, "A Comparative Study of the Recent Trends in Biometric Signature Verification", DOI: 10.1109/IC3.2013.6612219.(2014).
17. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
18. "Behavioral Biometrics", International Biometrics + Identity Association.
19. Roman V. Yampolskiy, Venu Govindaraju, "Strategy-based behavioural biometrics: a novel approach to automated identification", Int. J. Computer Applications in Technology, Vol. 35, No. 1, (2009).
20. Abhishek Sharma and Suresh Sundaram, "On the Exploration of Information From the DTW Cost Matrix for Online Signature Verification", IEEE (2017).
21. Abhishek Sharma and Suresh Sundaram, "A novel online signature verification system based on GMM features in a DTW framework", IEEE Transactions On Information Forensics and Security, (2016)
22. http://desktop.arcgis.com/en/arcmap/latest/tools/spatial-analyst-toolbox/train-random-trees-classifier.htm
23. Ranjan Kumar Singh, "Static Signature Authentication based on J48 and Random Forest", International Journal of Engineering Research & Technology (IJERT)(2017).
24. https://machinelearningmastery.com/logistic-regression-for-machine-learning/
25. https://www.dataschool.io/simple-guide-to-confusion-matrix-terminology/
26. Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira, "Learning Features for Offline Handwritten Signature Verification using Deep Convolutional Neural Networks", Pattern Recognition (2017), doi: 10.1016/j.patcog.2017.05.012
27. Luiz G. Hafemann, Robert Sabourin, Luiz S. Oliveira, "Analyzing features learned for Offline Signature Verification using Deep CNNs", In: 23rd International Conference on Pattern Recognition (ICPR), Cancún Center, Cancún, México (2016)
28. A. Namboodiri and S. Gupta, "Text independent writer identification from online handwriting" In: Proc. 10th Int. Workshop Front. Handwriting Recognition, pp. 287–292, (2006).
29. Y. Liu, Z. Yang, L. Yang, "Online signature verification based on DCT and sparse representation", IEEE Transactions on Cybernetics, vol. 45, no. 11, pp. 2498–2511(2015).
30. Andreas Fischer, Moises Diaz, Rejean Plamondon, Miguel A. Ferrer, "Robust Score Normalization for DTW-Based On-Line Signature Verification" In: 13th International Conference on Document Analysis and Recognition (ICDAR), (2015).
31. Sadhna, Ankita Sharma, "Human Behaviour Modelling & Analysis Using Artificial Neural Network" In: International Journal of Advanced Research in Computer Science and Software Engineering, (2015).
32. Ishan Bhardwaj, Narendra D. Londhe & Sunil K. Kopparapu (2016), " A Novel Behavioural Biometric Technique for Robust User Authentication,", IETE Technical Review, DOI: 10.1080/02564602.2016.1203271
33. Sukhdeep Singh, Dr. Sunil Kumar Singla, "A Review on Biometrics and Ear Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (2013).
34. K. Cpałka, "A new algorithm for identity verification based on the analysis of a handwritten dynamic signature", Appl. Soft Comput. J. http://dx.doi.org/10.1016/j.asoc.2016.02.017(2016).
35. Ioannis Rigas, George Economou, Spiros Fotopoulos, "Human eye movements as a trait for biometrical identification", IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS 2012).
36. Munish Sabharwal, "Contemporary Research: Intricacies and Aiding Software Tools Based on Expected Characteristics" AIMA Journal for Management & Research, ISSN:0974-497 Vol.10, Issue 2/4, pp. 1-16, March, 2016.
37. Presented Paper, "The use of soft computing technique of Decision Tree in selection of appropriate statistical test for Hypothesis Testing" in the "International Conference on Soft Computing: Theories and Applications (SoCTA 2016)" organized by Amity University, Jaipur, India on December 28-30, 2016, Proceedings in AISC series of Springer Indexed in SCOPUS (Elsevier).

AUTHORS PROFILE

Shalini Dhiman received her bachelor Engineering in Computer Science from Chitkara University, Baddi, H.P. in 2016. She is currently a M.E. student in Chandigarh University since 2017. Her research interest is in Artificial Intelligence and Machine learning.

Munish Sabharwal Qualified PhD (CS), PhD (Management) and contributing over 20+ years in Teaching (CS and MIS), Education Management, Re-search as well as S/W Development. Currently spearheading efforts as Professor (CSE) & Associate Dean, Chandigarh University, Mohali (Punjab) INDIA. Current research interests include Data Science, Biometrics & E-Banking.