



Online Signature Classification based on Dynamic Nature of Features Selection Framework

Akhilesh Kumar Singh¹, Surabhi Kesarwani², Anushree³, Pawan Kumar Verma¹, Nitin Rakesh⁴ and Monali Gulhane⁴

¹Sharda University, Greater Noida Uttar Pradesh, India

²Greater Noida Institute of Technology (Engineering Institute), Uttar Pradesh, India

³GLA University, Mathura, Uttar Pradesh, India

⁴Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Maharashtra, India

Received Mon. 20, Revised Mon. 20, Accepted Mon. 20, Published Mon. 20

Abstract: In recent digital age, online signature verification plays a key role in authentication including security standards across many industries, such as financial, legal, and ecommerce. The World Bank's data shows the global digital economy is growing fast, with internet usage nearly 60% of people worldwide. According to numbers from the International Telecommunications Union, over 4.7 billion individuals have become internet users with so many user doing internet's online, security and trust for online transactions are important issues. Forensics and biometrics are emerging as key players in this area. Verifying signatures digitally is one important use. As in the study mentioned earlier, using machine learning can help make signature verification systems more accurate and reliable. Our study describes an online verification method using machine learning that is based on the dynamic features of a signature and compares the outcomes to methods already in use. The online signature verification has been validated using supervised learning (K-nearest neighbour (KNN)). This research aimed to enhance authenticity and reduce the occurrence of false positives as its primary objectives. The outcomes show that this methodology has better authenticity than the current methods. The Signature Verification System (SVS) 2004 based signature data-sets is utilized in the tests.

Keywords: Online Signature Verification, Signature features, KNN (k Nearest Neighbor), Machine Learning

1. INTRODUCTION

Biometric systems have arisen as innovative security solutions in pattern recognition and E-systems, thanks to the rapid progress of information technology. Physiological and behavioural biometric systems are the two primary categories of biometric systems [1]. Physiological features are distinct human body properties that are static [2], [3]. Behavioural characteristics, on the other hand, are fluid and can change over time depending on mood, age, and other circumstances. Behavioral qualities are influenced by gait, signature, handwriting, voice, keyboard, and other modalities. The use of a handwritten signature is widely accepted by institutional and financial institutions as a reliable method of personal recognition [4], [5]. The commercial and banking sectors, as well as many other businesses, are now quickly utilizing digital signature systems that were created specifically to permit purchases and transfers. Signatures represent human biometrics that can vary because of certain conditions, such as age, mood, and climate so that two individual signatures cannot fit each other exactly [6]. The Signature Verification System, also called SVS,

recognises and validates a handwritten signature of authenticity. Static (offline) and dynamic SVS are two types of SVS (online). User signatures are digitised using a scanner or a camera from paper in an offline system, whereas they are digitised using a scanner or a camera in an online system [7]. The stability of dynamic features is minimized in most existing online handwritten signature authentication systems since they compare different signatures using the same homogenous feature sets for different nonidentical users [5], [8].

Enrollment and verification phases are common in on-line signature verification systems. Users supply their own self-reference-based signatures during the enrolling process, which are then included in a system that make use of feature extraction methods. The system compares and analogizes a signature query onto reference-dependent signatures and applies matching algorithms to approve or repudiate it during the verification phase [9]. The signature verification system's efficiency can be improved by focusing on feature extraction and classification methodologies. In online-based signature verification, feature extraction approaches



can be divided into parameterized and functionality-based approaches. Those that employ function-based strategies typically outperform systems that employ parameter-based techniques [10], [11].

Instance-based learning builds theories based on training and preparatory instances. Memory-based learning or sluggish learning are two terms used to describe it [12]. The time complexity of this technique is determined on how big the training data is. The determined time complexity for worst case approach on this methodology is $O(k)$, where, k is the count of training cases [13], [14].

But in today's world, the most vital and prime challenge with signature verification is signature variability. When signing one's name repeatedly, there may be some variation. This is because a handwritten signature is the result of an iterative generation process that can be difficult and depends on the signer's psychophysical state, as well as the circumstances in which the signature is written. The primary objective of this study is to evaluate and enhance the performance of the system, for dynamic signature verification in a compatible environment. We are concentrating on online signature verification, which involves determining if an online signature matches the claimed identity or not.[15].

A machine learning-based approach has been introduced for verifying online signatures that makes use of several dynamic features of signatures. The following are the main contributions of this paper:

- 1) An innovative technique has been suggested for the verification of signatures through the KNN classifier in an online setting.
- 2) The proposed method is more resilient since the extracted feature uses fewer resources.
- 3) We consider the dynamic features like, x-coordinate, y-coordinate, height, pressure, displacement, velocity, time stamp, pen up and down, azimuth, acceleration, etc., to make online signature more effective.
- 4) Experimental contribution and results depict that the proposed methodology and strategy is superior to existing traditional formulations in terms of achieving lower, i.e., reduced Understanding of the rates of false positives and false negatives is crucial for accurate decision making. In statistics and machine learning, these rates help to determine the reliability of a given model or test. By evaluating and minimizing these rates, we can improve the accuracy and effectiveness of our methods. Therefore, it is important to pay close attention to false positive and false negative rates to make informed and effective decisions.

The outline of the paper is explained as follows: the second section covers related work. Section 3 deals with signature verification processes and provides a concise overview of the database, feature extraction procedure,

and classifier. Section 4 presents experimental results and compares them with the current state-of-the-art method. Section 5 addresses the scope of future research.

2. LITERATURE

There are numerous known techniques for online verification systems. Some of the latest advancements in instance-based learning are discussed in this section.

Yang et al. [8] suggested a dynamic signature verification approach based on integrated stable characteristics. Training and testing are the two phases of the verification process for each user. The experiment is carried out on SVC2004 and their database. Only English and Chinese are used in this dataset. The proposed system has a lower FAR and FRR than other state-of-the-art strategies, according to experimental results. A smartphone-based safe and dynamic handwritten signature verification method was suggested by Xia et al. [16]. Both global and regional characteristics are extracted for verification purposes. In this case, kNN is utilised to secure the template and feature vector. The SG-NOTE database from a Samsung Galaxy Note and the MCYT-100 database from a WACOM pen tablet are used to demonstrate the output of the suggested technique [15].

Doroz et al. [4] describe a new signature verification method, assessing signature stability after verification. Fuzzy sets are utilized to identify the stable parts of signatures. Seven classifiers, including PSO orientated, The list below comprises some of the common machine learning algorithms: Naive Bayes, k-Nearest-Neighbor, Random Forest, SVM, RIDOR, and J48. were employed to assess the efficacy of this approach on the SVC2004 and MCYT databases. Additionally, a texture-based signature authentication method is suggested, which incorporates offline signatures in two distinct Indian scripts. [13].

Chandra et al. [17] A novel method for online signature validation using machine learning with six classifiers (NaiveBayes, PART, J48, MLP, Logistic, random forest) is proposed. The experiment is conducted on the SVC2004 dataset, utilising characteristics such as x and y coordinates for signature segmentation. Additionally, an approach for automatic offline handwriting signature recognition is recommended in [18] employing LBP and BSIF. This method is tested on the MCYT-75 and GPDS-100 datasets. For the MCYT-75 and GPDS-100 datasets, the k-nearest neighbor classifier achieves recognition accuracy of 97.3% and 96.1% respectively.

Upadhyay et al. [19] conducted a comparison analysis in order to assess the accuracy of signature verification schemes. The performance analysis is done using SVM and KNN techniques on the same dataset. The experimental findings show that SVM has higher accuracy but takes longer to perform (0.21 milliseconds). The accuracy of SVM and KNN is 88 percent and 76 percent, respectively, while the performance time of SVM and KNN is 0.21

milliseconds and 0.007 milliseconds, respectively. Azmi1 et al. [20] suggested an SVS system that utilises the Freeman chain code (FCC) for data representation. The FCC was obtained through a boundary-based approach on the largest contiguous area of the signature images in the first stage of feature extraction. [16]. Six global features were computed on a segmented image in the second phase to evaluate feature effectiveness. Subsequently, verification was computed and compared using k-nearest neighbours with Euclidean distance. [21]. Offline handwritten signature verification using Geodesic Derivative Pattern (GDP) is demonstrated [11], [22]. Geodesic distance and Local Derivative Pattern (LDerivP) are the features utilised in this study. The method is evaluated using the GPDS960Gray Signature database. A single genuine sample per participant was utilised to train a KNN model, while the remaining samples were used for testing.

Durrani et al. [23] presented a strategy that uses a dynamic temporal warping mechanism to create a signature envelope. The envelope serves as the foundation for determining whether or not a signature is forged. On a conventional Japanese handwritten dataset, they just use fundamental attributes like the signature's X and Y coordinates [24].

3. PROPOSED APPROACH

Figure. 1 illustrates the overview of our proposed signature verification methodology. The input signature taken from a pen pen-based tablet is first through a feature extraction method where dynamic features are extracted. Subsequent to that we use a classifier to compare it against from the trained signature database of the enrolled reference signatures of an user. Here, based on matching it classifies whether the test signature is genuine or forge.

A. Signature Database

The dataset used for evaluation is publicly available standard dataset consisting of English and Chinese signature which is used for Signature Verification Competition in 2004 (SVC2004) [25]. The set consist of collection of all forged and genuine type signature. The set contain information such as {x axis-coordinates, y axis-coordinate valued timestamp, pen in up and in pen down, pressure,height and azimuth} of each signature. In the current said framework the setup contains 200 signatures used for experiment and research, 100 each for genuine and forge.

B. Dynamic Signature' Features

The signatures of the individuals were taken throughout the process at each location. Edge points were used to record data during the sampling process. The SVC2004 signature gathers information such as x, y, date and time, pen vertically and horizontally, movement, speed, angle, altitude, force, and acceleration. Concatenating these features results in the feature vector $FV=X1$ to $X10$, which is utilised for training and testing.

The set $A = a1$ to a_n , where n is the total number of users,

serves as a representation of the pressure experienced by all users. In this situation, n is equal to 200. The symbol is then used to indicate the determined value. The same method is applied in several ways. Figures 4 and 5 show examples of authentic and counterfeit signatures, respectively.

By mixing several approaches, Weka's machine learning develops a model for training data. Table 1 demonstrates how three different learning algorithms are fed the chosen features.

TABLE I. Classifiers and learning types

Sl. No.	Classifier	Learning Type
1	Bayes-Net (BN)	Bayes
2	J48 (C4.5)	Decision Tree
3	MLP	Function
4	Naive-Bayes Net (NB Net)	Bayes
5	PART	Rules
6	Random-Forest (RF)	Decision Tree
7	Random-Tree (RT)	Decision Tree

1) Naive Bayes

Naive Bayes classifiers, which are straightforward probabilistic classifiers, are produced using the Bayes theorem. Using more sophisticated methods like support vector machines, it is a well-liked text categorization tool. An authentic signature can be distinguished from a false one using the Bayes rule.

Naive Bayes classifiers are extremely scalable because they require a lot of linear parameters. Evaluation of a closed-form expression is needed for maximum likelihood training utilising linear training as opposed to expensive iterative approximation.

2) J48

J48 is a classifier that learns via decision trees. Using the training dataset S, it developed a decision tree. The training dataset has been divided into subsets. J48 breaks down each node of the tree into subsets based on the signature class (genuine or forged) as shown in figure 2 and 3. The intent is to adapt a decision tree progressively until it reaches an optimal level of flexibility and precision.

3) MLP

A model for artificial neural networks called MLP converts input data into a number of acceptable outputs. It is composed of many layers of directed graph nodes, each of which is completely connected to the layer below it. For training, MLP employs back-propagation a supervised learning approach.

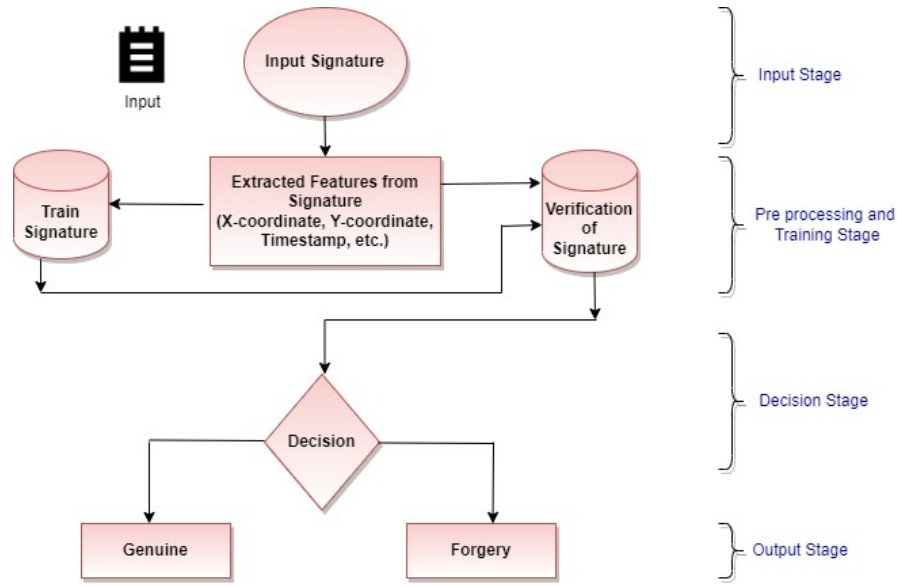


Figure 1. The proposed signature verification methodology

4) *PART*

A post-pruning tree classifier is PART. Prior to branch trimming and level determination for the decision tree, the trees must first be constructed. As a result, things become less complicated and easier to comprehend. Statistical techniques are employed to eliminate the least reliable branches, resulting in faster classification and reliably categorised test data [19].

5) *Bayes Net*

To get around the data reliance, a Bayesian network is used. This graphical layout can be used to illustrate and analyse a complex area. Each node in a Bayesian network corresponds to a feature that was randomly chosen from the feature collection. To demonstrate how characteristics are interconnected, a collection of directed interconnections are connected to pairs of nodes. The likelihood function for each node was used to measure the efficacy of the feature set. Directional cycles are not permitted in a Bayesian network, and that is all that is required.

6) *Random-Forest*

A random-forest (RF) is made up of several diversified trees. It works well with large databases. Without removing any of them, it can manage tens of hundreds of input variables. This gives an estimate of the variables that are essential to the classification. The generalisation mistake is generated internally and impartially as the forest expands [21]. To train the random forest classification, we used the S data. Each and every column signifies a different component of the data-sets, with the exception of the final column, which indicates the class of the signature.

4. RESULT AND FINDINGS

This part of the research article focuses on the proposed system’s experimental configuration, performance

measures, and experimental results in depth.

A. *Experimental Configuration*

The classifier in our experiment is fed the training data. Here, the selected characteristics are classified using the K closest neighbours classifier. With I = 1 to 10 as the feature set, we use the approach $M I = FV$.

An effective machine learning technique is called K nearest neighbours. It keeps track of all potential outcomes and classifies new ones using distance measures as a cosine similarity. By a majority vote of their neighbours, cases are classified correctly with the most participants among their K closest and nearest neighbor, as signified by a distance function. When K is 1, the case is simply put in the class of the closest neighbour. From data preparation through statistical assessing learning techniques to display of learning data and results, it offers complete assistance for the overall study data mining process.

B. *Performance Measures*

The performance evaluation [4], [26] of the proposed scheme is measured and analysed with respect to various evaluation metric shown and indicated in Table II.

TABLE II. Evaluation Measure

Eval. Measure	Equation
TP Rate	True Positive/(FN+TP)
FP Rate	False Positive/(TN+FP)
ACC	(TN+TP)/Total (N+P)
F-Score	$2TP/(FP+2TP+FN)$
MCC	$\frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$
AMER	Avg. Mean Error of FA Rate & FR Rate

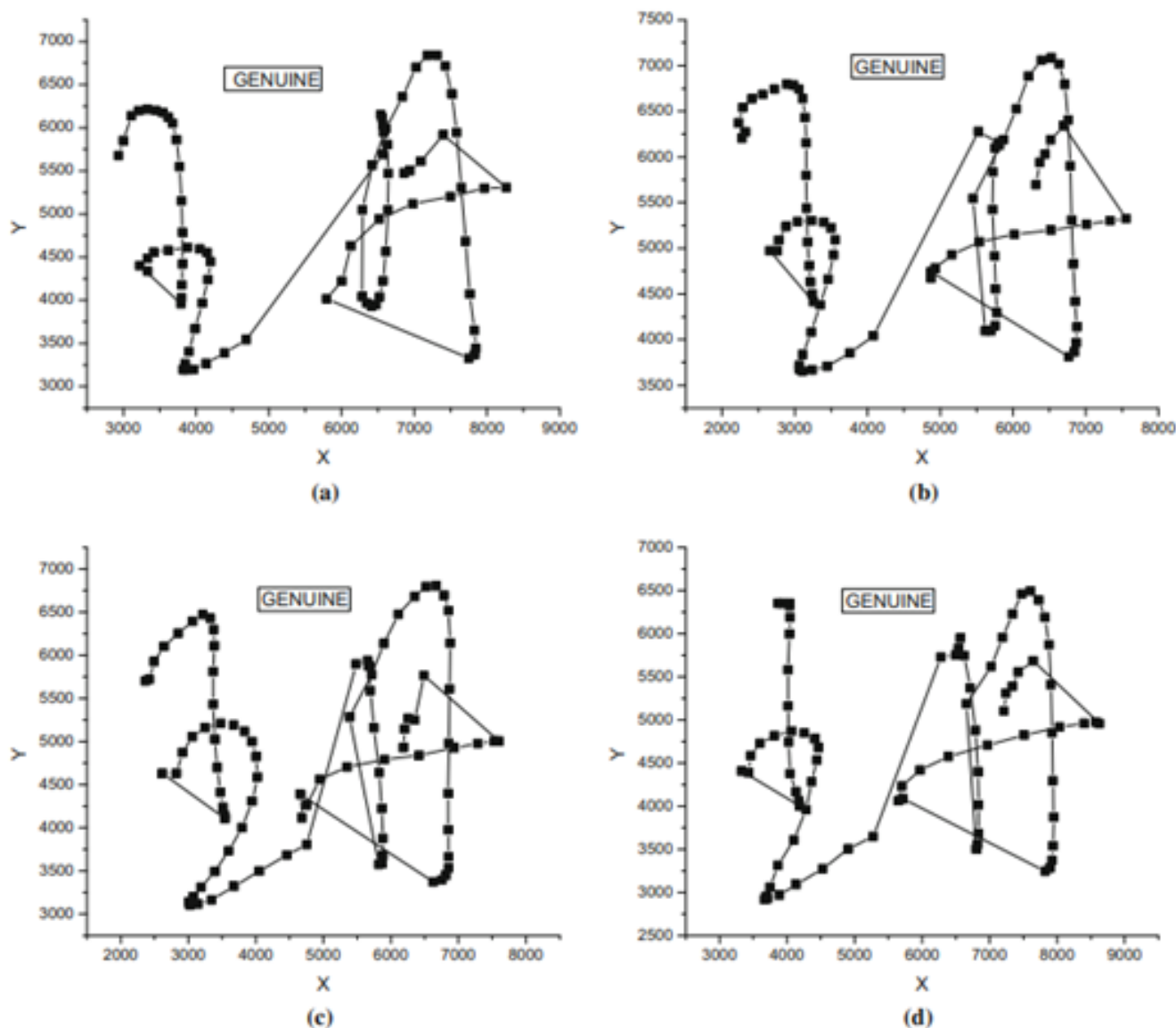


Figure 2. Genuine Signature sample (User1)

C. Experiment Performance Results

Following the extraction of features, the classifier is fed training data. The K Nearest Neighbors classifier receives the chosen characteristics as input. $M_i = FV$, i counts 1 to 10, is the feature set used in this approach. True positive, false positive, true negative, and false negative are the specifics of the confusion matrix as shown in Table.3. Users 1 have 100% TP and TN. User 3's TN is 100% and TP is 99.9% in this situation. But as compared to Users 2 and 4, User 5's measurements of TP and TN were lower.

where, TP, FN, TN and FP have their usual meanings of True Positive, False Negative, True Negative and False Positive

TABLE III. Measured values of confusion matrix

Parameter	User ₁	User ₂	User ₃	User ₄	User ₅
TP	3230	3554	4512	6576	3273
FN	0	4	1	48	45
TN	5019	7125	4807	8221	5288
FP	0	11	0	60	38

The statistical value derived from various users is displayed in Table IV in this article. User 1, followed by

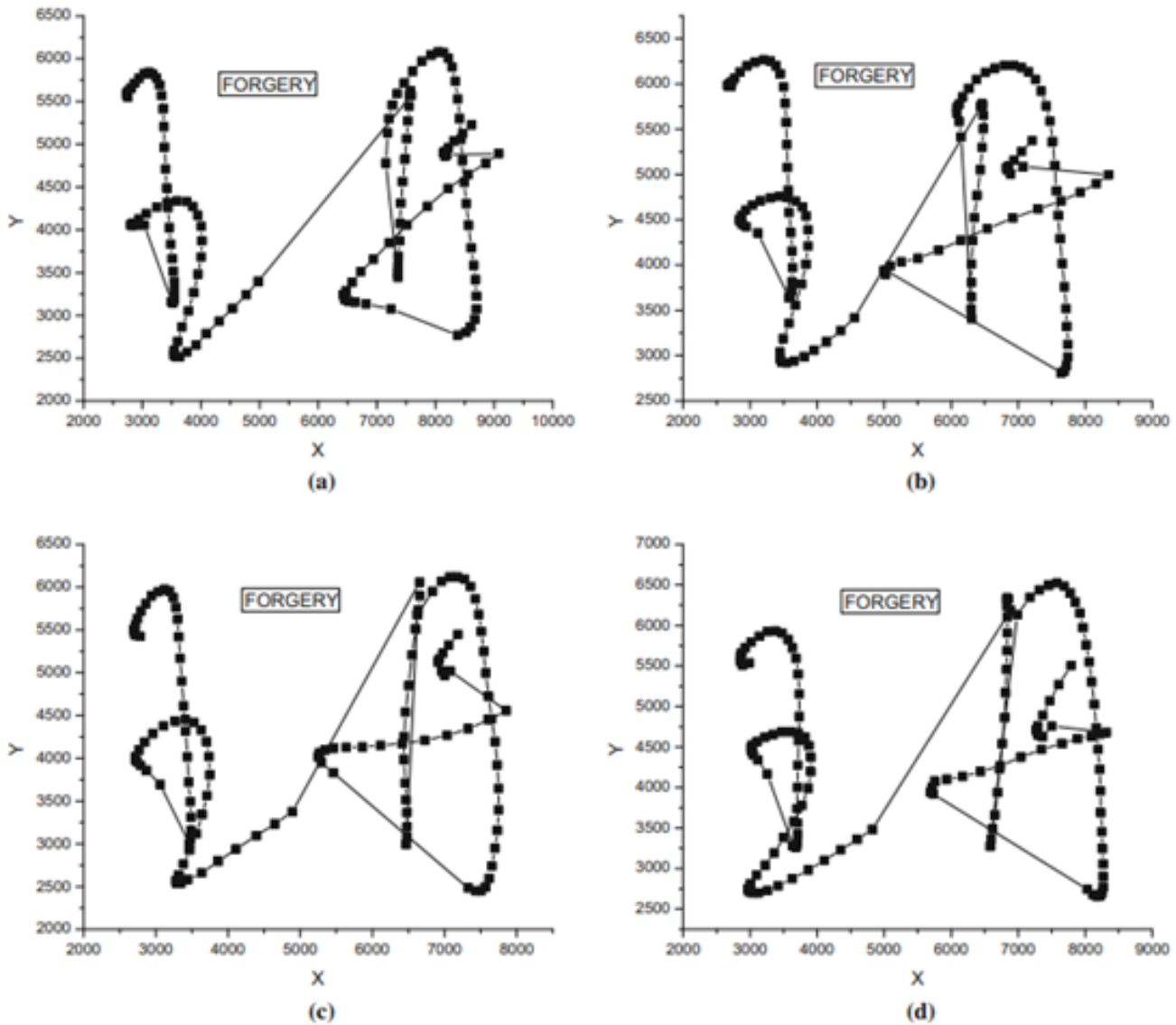


Figure 3. Forgery Signature sample (User1)

User 3 and User 2, with an accuracy rate of one cent. The accuracy rate measured by User 5 is lower compared to User 4 nonetheless. User 1 outperforms the other users in terms of many types of error that includes relative absolute error (RAE), root average mean squared error (RAMSE) and root relative squared error (RRSE).

Table V displays the complete parameter computation for each of the five users. Here, signatures are divided into categories for real and fake ones. We infer from the table that User1 is more accurate in comparison to other users. If we take a closer look, we can see that all users' FPR values for the counterfeit category are higher than those for the genuine class (G) and 'F' denotes forgery class this is represented as '*'.

Figures 4 and 5 show the details of User 1's fake and real signatures, each with a different set of characteristics. Figure.4 shows that when the number of cases rises, the FPR and fallout both drop. The F-measure behaves similarly, but it increases in the middle position before curving downward. After a few iterations, precision and lift of the forge signature grow according to the instance count, while fallout and precision remain unchanged. The lift and precision of signature classified as genuine, as shown in Fig. 5, are observed to grow with respect to the number of occurrences while remaining constant after a number of iterations in the case of User1's genuine signature, as demonstrated. F-measure and FPR show a certain number of instances of decreasing. As a result, we deduce from User 1's Fig.4

TABLE IV. Measured statistical values

Statistical variable	User ₁	User ₂	User ₃	User ₄	User ₅
Correct Classification	8249	10679	9319	14797	8561
Incorrect Classification	0	15	1	108	83
Kappa measured statistic	1	0.9968	0.9998	0.9853	0.9797
M A Error	0.0001	0.0015	0.0002	0.0073	0.0097
R M S Error	0.0001	0.0374	0.0104	0.0851	0.098
R A Error	0.0283	0.3392	0.0453	1.4822	2.0566
R A S Error	0.0276	7.9477	2.0726	17.1295	20.1466

TABLE V. Parameter calculation

User	TP Rate	FP Rate	Precision	Recall	F-Score	MCC	ROC area	PRC area	*
1	1.01	0.01	1.01	1.0	1.0	1.0	1.0	1.0	G
	1.01	0.01	1.01	1.01	1.0	1.0	1.0	1.0	F
2	0.999	0.002	0.997	0.999	0.998	0.997	0.998	0.996	G
	0.998	0.001	0.999	0.998	0.999	0.997	0.998	0.999	F
3	1.0	0.0	1.0	1.0	1.0	1.0	1.0	1.0	G
	1.0	0.0	1.0	1.0	1.0	1.0	1.0	1.0	F
4	0.993	0.007	0.991	0.993	0.992	0.985	0.993	0.987	G
	0.993	0.007	0.994	0.993	0.993	0.985	0.993	0.992	F
5	0.986	0.007	0.989	0.986	0.987	0.980	0.990	0.981	G
	0.993	0.014	0.992	0.993	0.992	0.980	0.990	0.990	F

and Fig.5 that all the parameters provide results that are essentially comparable when comparing authentic and fake signatures.

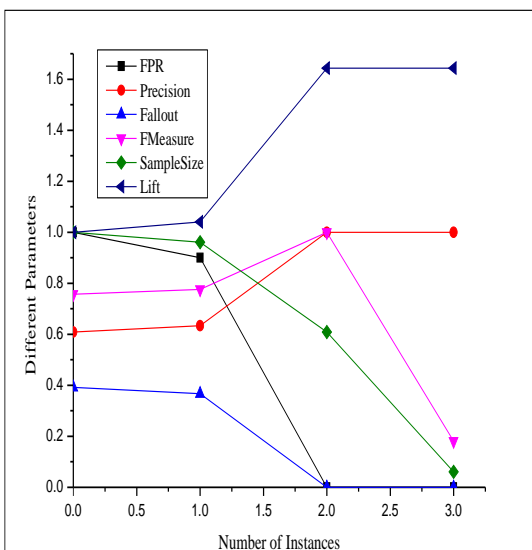


Figure 4. Performance of User₁ forgery signatures

Figures 6 and 7 exhibit the specifics of User 2’s fake and real signatures, respectively. In Fig. 6, we can see that, relative to the number of instances, the precision and lift are increasing while the F-measure, fallout, and FPR are decreasing. But in Fig. 7, lift, F-measure, and precision all

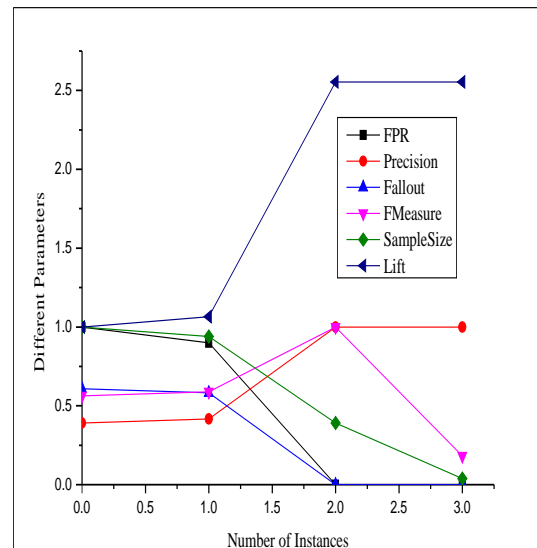


Figure 5. Performance of User₁ genuine signatures

rise linearly with respect to the number of instances, but fallout and FPR of the actual signature decline. We can therefore deduce from User 2’s Figs. 6 and 7 that the forgery set of signatures is more accurate than the real ones.

Fig. 8 and Fig. 9 demonstrate, respectively, the details of User 3’s fake and real signatures. Fig. 8 shows that while F-measure, fallout, and FPR decline relative to the number of instances, precision and lift grow and remain constant after several iterations. But in Figure 9, lift, F-measure, and precision all rise linearly with respect to the number of instances, whereas fallout and FPR of the actual signature decline. Thus, from User 3’s Figures 8 and 9, we deduce that after a certain number of iterations, the lift of a genuine signature improves exponentially compared to a collection of fake signatures.

Fig. 10 and Fig. 11 demonstrate, respectively, the details of User 4’s fake and real signatures. We can see in Fig. 10 that, similar to User3, precision and lift grow and remain constant after a number of iterations, however fallout and FPR decline according to the number of instances. Although

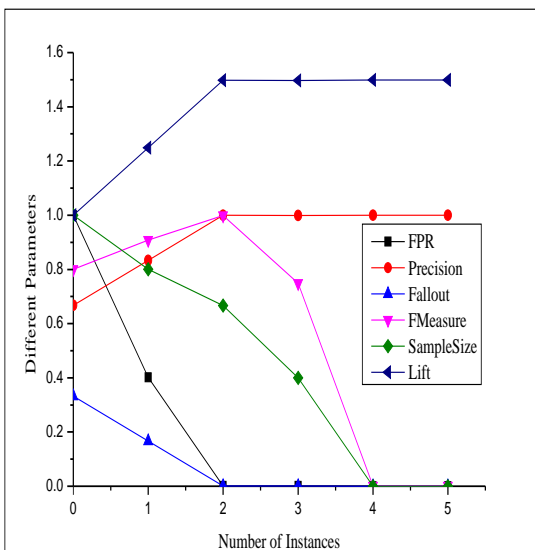


Figure 6. Performance of User₂ forgery signatures

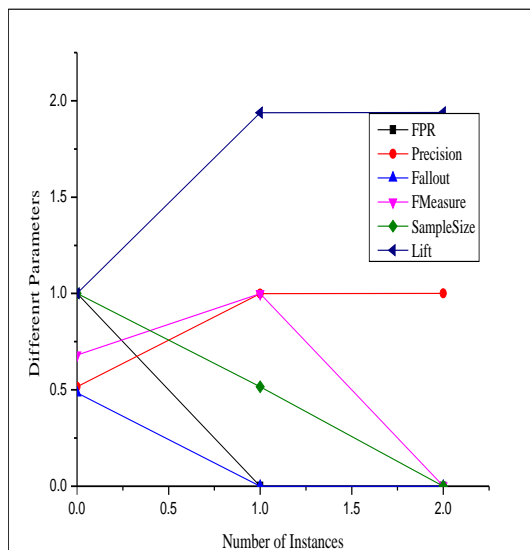


Figure 8. Performance of User₃ forgery signatures

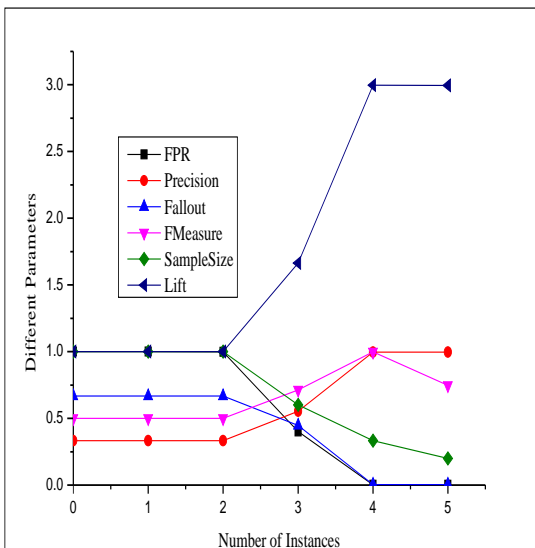


Figure 7. Performance of User₂ genuine signatures

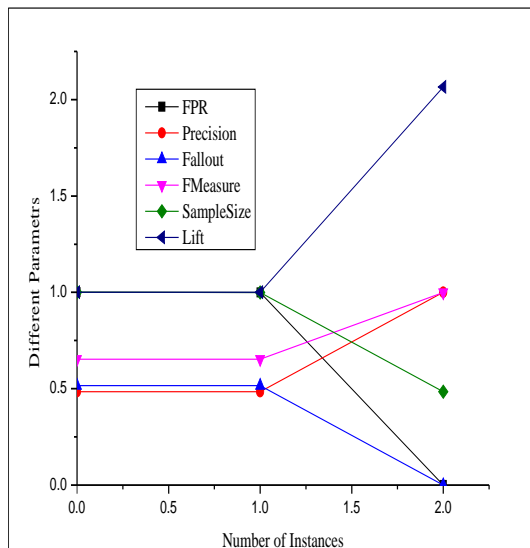


Figure 9. Performance of User₃ genuine signatures

F-Measure and FPR of the real signature decline according to the number of instances in Fig.11, precision, lift, and fallout increase first and then remain constant. Accordingly, given User 4’s Figures 10 and 11, we may infer that after a certain number of iterations, the consequences of a genuine signature rise in comparison to a set of fake signatures.

Figs. 12 and 13 demonstrate, respectively, the specifics of User 5’s fake and real signatures. In Fig. 12, we can see that, similar to User 4, the precision and lift grow and then remain constant over time, however the FPR declines

relative to the number of instances. However, in Fig. 13, while F-Measure and FPR of genuine signature decline relative to the number of instances, precision, lift, and fallout grow and then remain constant with time. Thus, based on User 5’s Figures 12 and 13, we deduce that after a certain number of iterations, the lift of a genuine signature increases exponentially compared to a set of forgeries.

The FRR and FAR of our suggested system based on the SVC2004 databases are shown in Table 6. The experimental results are based on three parameters: falsely rejected rate

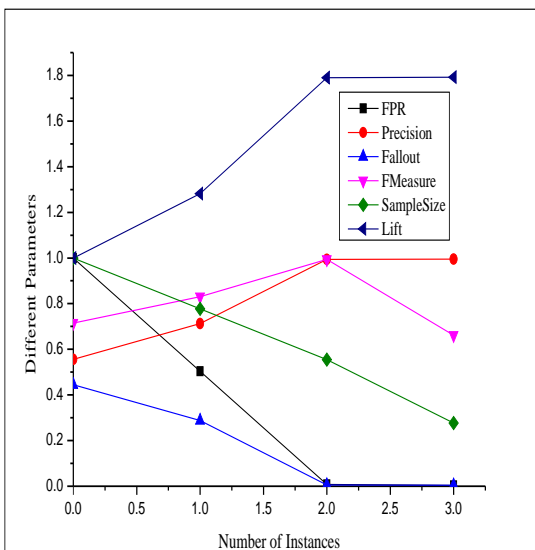


Figure 10. Performance of User₄ forgery signatures

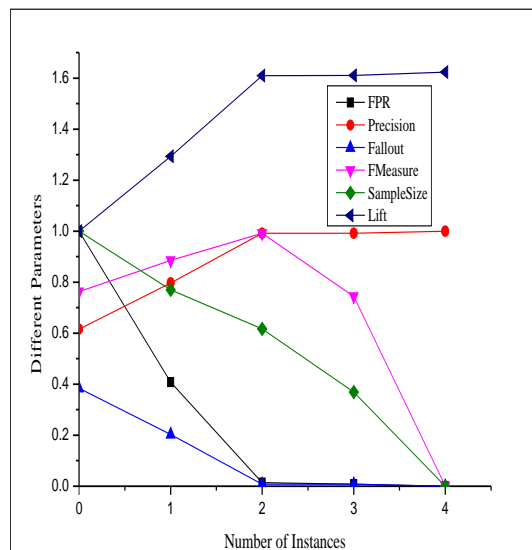


Figure 12. Performance of User₅ forgery signatures

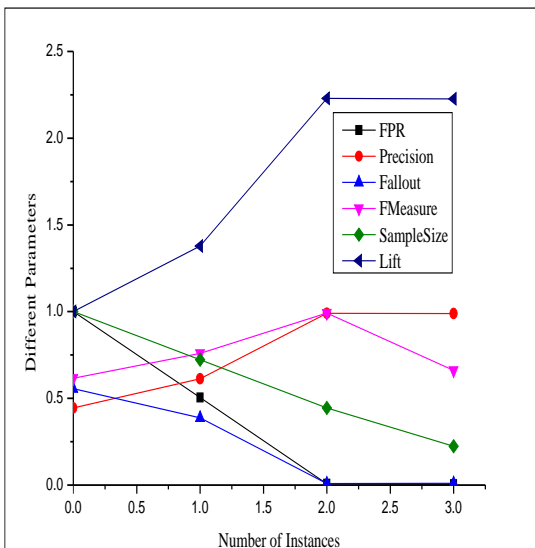


Figure 11. Performance of User₄ genuine signatures

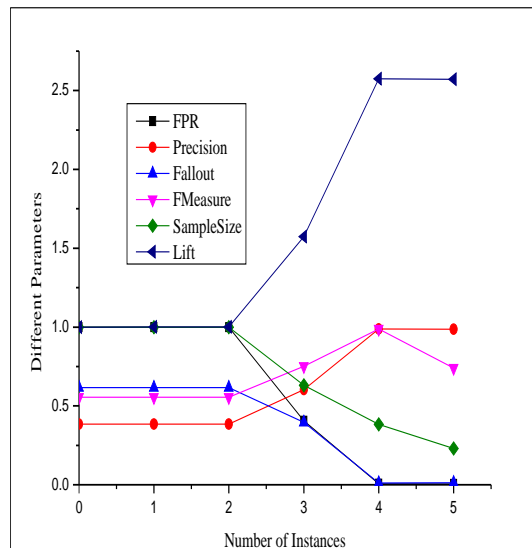


Figure 13. Performance of User₅ genuine signatures

(FRR), falsely accepted rate (FAR), and average mean error for FRR and FAR (AER).

Table 7 shows how different strategies are compared. In the current system, multiple ways use different databases. It is therefore impossible to make a reliable comparison between various approaches. However, our suggested method performs better than the current way in terms of output.

TABLE VI. FRR and FAR in Experiment

Users	FAR	FRR	AER
User ₁	0	0	0
User ₂	0	0.27	0.13
User ₃	0	0	0
User ₄	0.24	0.02	0.13
User ₅	0.05	0	0.025
Average	0.058	0.058	0.26



TABLE VII. Performance of the proposed scheme

The Approach	FRR	FAR	Dataset
Yang et al. [27]	5.5	5.125	SVC2004
Chandra et al. [17]	5.76	6.25	SVC2004
Chandra [26]	2.619	2.619	SVC2004
Proposed Curent Method	0.0579	0.0579	SVC2004

5. CONCLUSION

Proposed KNN-based machine learning technique has been successfully used to perform online verification using the dynamic parameters of the signature with greater accuracy. This innovative method distinguishes between false and real signatures with a 98 percent accuracy. The results were compared with those of currently existing technologies or methodologies using the standard dataset. In our tests, we obtained False Acceptance Rates of 0.058 and False Rejection Rates of 0.058, which are significantly better outcomes than those obtained using existing techniques. The real-time system can benefit from this verification algorithm. Velocity, azimuth, X and Y axis coordinates, acceleration, pressure, time stamp, displacements, pen up and pen down, etc. are examples of dynamic features that have been measured. Increasing the dynamic features for the verification purpose is also a cause to get the better accuracy and reduce the False positive rate.

REFERENCES

- [1] K. Bibi, "Saeeda naz and arshia rehman." "biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities." *Multimedia Tools and Applications*, vol. 79, no. 1, pp. 289–340, 2020.
- [2] R. Agarwal, "Local and global features based on ear recognition system," in *International Conference on Artificial Intelligence and Sustainable Engineering*. Springer, 2022, pp. 477–486.
- [3] R. K. Tripathi and A. S. Jalal, "Novel local feature extraction for age invariant face recognition," *Expert Systems with Applications*, vol. 175, p. 114786, 2021.
- [4] R. Doroz, P. Kudlacik, and P. Porwik, "Online signature verification modeled by stability oriented reference signatures," *Information Sciences*, vol. 460, pp. 151–171, 2018.
- [5] D. Impedovo and G. Pirlo, "Automatic signature verification in the mobile cloud scenario: survey and way ahead," *IEEE Transactions on Emerging Topics in Computing*, 2018.
- [6] M. Houtinezhad and H. R. Ghaffary, "Writer-independent signature verification based on feature extraction fusion," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 6759–6779, 2020.
- [7] A. N. Azmi, D. Nasien, and F. S. Omar, "Biometric signature verification system based on freeman chain code and k-nearest neighbor," *Multimedia Tools and Applications*, vol. 76, no. 14, pp. 15 341–15 355, 2017.
- [8] L. Yang, Y. Cheng, X. Wang, and Q. Liu, "Online handwritten signature verification using feature weighting algorithm relief," *Soft Computing*, vol. 22, no. 23, pp. 7811–7823, 2018.
- [9] T. Hafs, L. Bennacer, M. Boughazi, and A. Nait-Ali, "Empirical mode decomposition for online handwritten signature verification," *IET Biometrics*, vol. 5, no. 3, pp. 190–199, 2016.
- [10] Y. Liu, Z. Yang, and L. Yang, "Online signature verification based on dct and sparse representation," *IEEE transactions on cybernetics*, vol. 45, no. 11, pp. 2498–2511, 2014.
- [11] M. Okawa, "Time-series averaging and local stability-weighted

- dynamic time warping for online signature verification,” *Pattern Recognition*, vol. 112, p. 107699, 2021.
- [12] V. Sharma, A. Chauhan, H. Saxena, S. Mishra, and S. Bansal, “Secure file storage on cloud using hybrid cryptography,” in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*. IEEE, 2021, pp. 1–6.
- [13] S. Pal, A. Alaci, U. Pal, and M. Blumenstein, “Performance of an off-line signature verification method based on texture features on a large indic-script signature dataset,” in *2016 12th IAPR workshop on document analysis systems (DAS)*. IEEE, 2016, pp. 72–77.
- [14] S. Schaal, C. G. Atkeson, and S. Vijayakumar, “Real-time robot learning with locally weighted statistical learning,” in *Proceedings 2000 ICRA. Millennium Conference. IEEE International Conference on Robotics and Automation. Symposia Proceedings (Cat. No. 00CH37065)*, vol. 1. IEEE, 2000, pp. 288–293.
- [15] P. Englert, “Locally weighted learning,” in *Seminar Class on Autonomous Learning Systems*. Citeseer, 2012.
- [16] Z. Xia, T. Shi, N. N. Xiong, X. Sun, and B. Jeon, “A privacy-preserving handwritten signature verification method using combinatorial features and secure knn,” *IEEE Access*, vol. 6, pp. 46 695–46 705, 2018.
- [17] S. Chandra, K. K. Singh, S. Kumar, K. Ganesh, L. Sravya, and B. P. Kumar, “A novel approach to validate online signature using machine learning based on dynamic features,” *Neural Computing and Applications*, pp. 1–20, 2021.
- [18] H. Hezil, R. Djemili, and H. Bourouba, “Signature recognition using binary features and knn,” *International Journal of Biometrics*, vol. 10, no. 1, pp. 1–15, 2018.
- [19] A. Upadhyay, S. Nadar, and R. Jadhav, “Comparative study of svm & knn for signature verification,” *Journal of Statistics and Management Systems*, vol. 23, no. 2, pp. 191–198, 2020.
- [20] S. Abdoli and F. Hajati, “Offline signature verification using geodesic derivative pattern,” in *2014 22nd Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 2014, pp. 1018–1023.
- [21] P. K. Singh, S. Sinha, and P. Choudhury, “An improved item-based collaborative filtering using a modified bhattacharyya coefficient and user–user similarity as weight,” *Knowledge and Information Systems*, vol. 64, no. 3, pp. 665–701, 2022.
- [22] M. Raj and A. K. Singh, “Humanoid gait pattern generation with orbital energy,” *Journal of Circuits, Systems and Computers*, vol. 30, no. 14, p. 2150259, 2021.
- [23] M. Y. Durrani, S. Khan, and S. Khalid, “Versig: a new approach for online signature verification,” *Cluster Computing*, vol. 22, no. 3, pp. 7229–7239, 2019.
- [24] J. Schneider and A. W. Moore, *A locally weighted learning tutorial using vizier 1.0*. Carnegie Mellon University, the Robotics Institute, 2000, vol. 149.
- [25] D.-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, “Svc2004: First international signature verification competition,” in *International conference on biometric authentication*. Springer, 2004, pp. 16–22.
- [26] S. Chandra, “Verification of dynamic signature using machine learning approach,” *Neural Computing and Applications*, pp. 1–21, 2020.
- [27] L. Yang, Y. Cheng, X. Wang, and Q. Liu, “Online handwritten signature verification using feature weighting algorithm relief,” *Soft Computing*, vol. 22, no. 23, pp. 7811–7823, 2018.



Akhilesh Kumar Singh currently working as an Assistant Professor in the Department of CSE in the School of Engineering & Technology, Sharda University. I have completed my M. Tech from IIT in Computer Science domain. Currently I am pursuing part time Ph.D. in Computer Science from NIT GOA. My area of interest lies in IOT, Networks and Operating System. Currently I have more than 45 research papers published that includes 6 SCI, 20 Scopus journal articles and rest all Scopus based conference. I have also published 6 patents, granted 2 patents and published 4 book chapters.



Surabhi kesarwani has more than 13 years of experience in academic and administration. During her academic tenure she has published various research articles in reputed national and international journals and conferences. She has also been granted many patents for her innovative work in research. Her area of interest includes data science and machine learning.



Anushree is an Assistant Professor at GLA University, Mathura. She has published more than 10 papers in international journals and conferences of repute. Her research areas include Software Engineering, Software Testing, and Artificial Intelligence.



Dr. Pawan Kumar Verma is an accomplished professional in the field of Computer Science and Engineering, with a strong focus on Machine Learning. He serves as an Associate Professor in the CSE department and is recognized as a skilled ML researcher. He has a prolific academic record with multiple publications, including 1 IEEE Transactions paper, 6 papers in SCIE-indexed journals, 6 papers in Scopus-indexed journals, and 3

papers in ESCI-indexed journals. His expertise extends to Java programming, as evidenced by his certification as a Wipro Certified Java Trainer. With a professional journey spanning 11.5 years, Dr. Verma has amassed a wealth of experience and knowledge.



Nitin Rakesh is a recipient of IBM Drona Award and Top 10 State Award Winner. He is active member of professional society like Senior Member IEEE (USA), ACM, SIAM (USA), Life Member of CSI and other professional societies. He is reviewer of several prestigious Journals/Transactions like IEEE Transactions on Vehicular Technology, The Computer Journal, Oxford Press, many SPRINGER/other Scopus indexed International Journals. He has published more than 200 SCI/Scopus Journal/Conference publication high quality journals and conferences. Dr Nitin is having more than 90 patents/innovations/designs in his credentials.

Dr Nitin is having more than 90 patents/innovations/designs in his credentials.



Monali Gulhane is recipient of young researcher award in 2021 by INSC, she has been merit holder in academics and received M.Tech in Computer Science Engineering from G. H. Rasoni College of Engineering and Technology for Women's (G.R.C.E.T.W), Nagpur, Maharashtra, in 2012-2014. She is currently pursuing PhD degree in Artificial Intelligence and Machine Learning from Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. She has published patents, copyrights, and technical articles..

She has published patents, copyrights, and technical articles..