International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Sep-24)

http://dx.doi.org/10.12785/ijcds/160197

Online Signature Classification Based on Dynamic Nature of Features Selection Framework

Akhilesh Kumar Singh[1], Surabhi Kesarwani[2], Anushree[3], Pawan Kumar Verma[1,*], Nitin Rakesh[4] and Monali Gulhane[4]

[1]*Sharda University, Greater Noida Uttar Pradesh, India*
[2]*Greater Noida Institute of Technology (Engineering Institute), Uttar Pradesh, India*
[3]*GLA University, Mathura, Uttar Pradesh, India*
[4]*Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, Maharashtra, India*

Received 15 Mar. 2024, Revised 27 May 2024, Accepted 31 May 2024, Published 15 Sep. 2024

Abstract: In the recent digital age, online signature verification plays a crucial role in authentication, including security standards across many industries, such as financial, legal, and e-commerce. Bank'srld Bank's data shows the global digital economy is growing fast, with internet usage for nearly 60% of people worldwide. According to numbers from the International Telecommunications Union, over 4.7 billion individuals have become internet users. With so much internet online, security and trust for online transactions are essential 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 based on a signature's dynamic features and compares the outcomes to methods already in use. The online signature verification has been validated using supervised learning (K-nearest neighbor (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 datasets are 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 behavioral biometric systems are the two primary categories of biometric systems [1]. Physiological features are distinct human body properties that are static [2], [3]. Behavioral 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. 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 treated specifically to permit purchases and transfers. Signatures represent human biometrics that can vary because of certain conditions, such as age, mood, and climate, so two individual signatures cannot fit each other exactly [6]. The Signature Verification System, also called SVS, recognizes and validates a handwritten signature of authenticity. Static (offline) and dynamic SVS are two types of SVS (online). User signatures are digitized using a scanner or a camera from paper in an offline system, whereas they are digitized 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 typical in online signature verification systems. Users supply their self-reference-based signatures during the enrolling process, which are then included in a system that makes 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 version system's efficiency can be improved by focusing on feature extraction and classification methodologies. In online-

Email: akhilesh.singh1@sharda.ac.in, surabhikesarwani.mca@gniot.net.in, anushree.gla@gla.ac.in, abes.pawan@gmail.com,nitin.rakesh@gmail.com,monaligulhane4@gmail.com

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 by how big the training data is. The determined time complexity for the worst-case approach on this methodology is $O(k)$, where k is the count of training cases [13], [14].

Today's world, the most vital and prime challenge with signature verification is signature variability. When one's name is repeated, there may be some variation. This is because a handwritten signature is the result of an iterative generation process that can be difficult and dependent 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 system's performance, 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 uses 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 are 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 essential to pay close attention to false positive and false negative rates to make informed and effective decisions.

The paper's outline 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

Numerous techniques for online verification systems exist. This section discusses some of the latest advancements in instance-based learning.

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 was carried out on SVC 2004 and its 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 utilized 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 is 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 SVC 2004 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, utilizing 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 utilizes 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 rst stage of feature extraction. [16]. Six global features were computed on a segmented image in the second phase to evaluate feature e ectiveness. Subsequently, veri cation was computed and compared using k-nearest neighbors with Euclidean distance. [21]. O ine handwritten signature veri cation using Geodesic Derivative Pattern (GDP) is demonstrated [11], [22]. Geodesic distance and Local Derivative Pattern (LDerivP) are the features utilized in this study. The method is evaluated using the GPDS960Gray Signature database. A single genuine sample per participant was utilized for training 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 attribute signature's X and Y coordinates [24].

3. Proposed Approach

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

A. Signature Database

The dataset used for evaluation is a publicly available standard dataset consisting of English and Chinese signatures, which was used for the Signature Veri cation Competition in 2004 (SVC2004) [25]. The set consists of a collection of all forged and genuine type signatures. The set contains 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 framework, the setup contains 200 signatures used for experiment and research, 100 each for genuine and forged.

B. Dynamic Signature Features

The individuals' signatures 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.

Extracting features play a crucial role in determining the veri ability of online signatures. The feature gathered in our proposed approach uses the SVC 2004 dataset that gathers information for features such as x, y, date and time, pen vertically and horizontally, movement, speed, angle, altitude, force, and acceleration. A detailed description of feature extraction of our proposed approach is shown in Table I .

TABLE I. Classi ers and learning types

Sl. No.	Feature Name	Description
1	x	Coordinate x(t)
2	y	Coordinate y(t)
3	Date and Time	dt(t)
4	Pen Vertically Horizontally	Absolute position, r(t); $p\sqrt{x^2(t) + y^2(t)}$
5	Movement	Acceleration in x $a_x(t)$, Acceleration in y $a_y(t)$
6	Speed	Velocity in x $v_x(t)$ Velocity in y $v_y(t)$
7	Angle	$v = tg^{1}\frac{v_y(t)}{v_x(t)}$
8	Altitude	al(t)
9	Force	p(t), $v_p(t)$
10	Acceleration	r(t), $a_r(t)$

Concatenating these features results in the feature vector FV=X1 to X10, which is utilized for training and testing. The set A= a1 to an, 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 apWeka's, Weka's machine learning develops a model for training data. Table II demonstrates how three di erent learning algorithms are fed the chosen features.

TABLE II. Classi ers and learning types

Sr. No.	Classi er	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 classi ers, which are straightforward probabilistic classi ers, are produced using the Bayes theorem. Using more sophisticated methods like support vector machines, it is a well-liked text categorization tool. An

Figure 1. The proposed signature veri cation methodology

authentic signature can be distinguished from a false one using the Bayes rule.

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

2) J48

J48 is a classi er 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 Figures 2 and 3. The intent is to adapt a decision tree progressively until it reaches an optimal level of exibility and precision.

3) MLP

A model for arti cial 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.

4) PART

A post-pruning tree classi er is PART. Prior to branch trimming and level determination for the decision tree, the trees must rst 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 classi cation and reliably categorized 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 analyze 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 accuracy 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 diversi ed 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 classi cation. The generalization mistake is generated internally and impartially as the forest expands [21]. To train the random forest classi cation, we used the S data. Each and every column signi es a different component of the dataset, with the exception of the nal column, which indicates the class of the signature.

4. Result and Findings

This part of the research article focuses on the system's system's experimental con guration, performance measures, and experimental results in depth.

A. Experimental Con guration

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

An e ective machine learning technique is called K nearest neighbors. It keeps track of all potential outcomes and classi es new ones using distance measures as cosine similarity. By a majority vote of their neighbors, cases are classi ed correctly with the most participants among their K closest and nearest neighbor, as signi ed by a distance function. When K is 1, the case is simply put in the

Figure 2. Genuine Signature sample (User1)

class of the closest neighbor. From data preparation through statistical assessment learning techniques to the display of learning data and results, it ers complete assistance for the overall study data mining process.

B. Performance Measures

The performance evaluation [4], [26] of the proposed scheme is measured and analyzed with respect to various evaluation metrics shown and indicated in table III.

C. Experiment Performance Results

Following the extraction of features, the classi er is fed training data. The K Nearest Neighbors classi er receives the chosen characteristics as inputM$_i$=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 speci cs of the confusion matrix as shown in table IV. Users 1 have 100% TP and 3's. User 3's TN is 100% and TP is 99.9% in this situation. But as compared to Users 2 an5's, User 5's measurements of TP and TN were

TABLE III. 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	$\frac{(TP\ TN\ FP\ FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$
AMER	Avg. Mean Error of FA Rate & FR Rate

Figure 3. Forgery Signature sample (User1)

lower.

TABLE IV. Measured values of confusion matrix

Parameter	User1	User2	User3	User4	User5
TP	3230	3554	4512	6576	3273
FN	0	4	1	48	45
TN	5019	7125	4807	8221	5288
FP	0	11	0	60	38

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

The statistical value derived from various users is displayed in table V in this article. User 1, followed by 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 including relative absolute error (RAE), root average mean squared error (RAMSE) and root relative squared error (RRSE).

Table VI displays the complete parameter computation for each of the ve 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 all users' FPR values for the counterfeit category are higher than those for the genuine class' 'G, and 'F' denotes the forgery class. This is represented as '*'.

TABLE V. Measured statistical values

Statistical variable	User1	User2	User3	User4	User5
Correct Classi cation	8249	10679	9319	14797	8561
Incorrect Classi cation	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 VI. 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

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, the precision and lift of the forged signature grow according to the instance count, while fallout and precision remain unchanged. The lift and precision of the signature classi ed 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 User1's of User1's genuine signature, as demonstrated. F-measure and FPR show a certain number of instances of decreasing. As a result, we deduce 1'sm User 1's Fig.4 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 speci cs 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 rise linearly with respect to the number of instances, but fallout and FPR of the actual signature decline. We can, therefore, deduce 2'sm User 2's Figs. 6 and 7 that the forgery set of signatures is more accurate than the real ones.

Figure 5. Performance of User1 genuine signatures

Fig. 8 and Fig. 9 demonstrate, respectively, the detail3'sf 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, 3'sm User 3's Figures 8 and 9, we deduce

Figure 6. Performance of User2 forgery signatures

Figure 7. Performance of User2 genuine signatures

Figure 8. Performance of User3 forgery signatures

Figure 9. Performance of User3 genuine signatures

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 detail4'sf 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 the 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, g4'sn 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 specific5'sf 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, base5'sn 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 VII. The experimental results are based on three parameters: falsely rejected rate (FRR), falsely accepted rate (FAR), and average mean

Figure 10. Performance of User$_4$ forgery signatures

Figure 11. Performance of User$_4$ genuine signatures

Figure 12. Performance of User$_5$ forgery signatures

Figure 13. Performance of User$_5$ genuine signatures

error for FRR and FAR (AER).

TABLE VII. 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 VIII shows how different strategies are compared. The proposed approach is compared with [27], [17] and [26] on same dataset. The falsely rejected rate (FRR) and falsely accepted rate (FAR) show an improvised result in our proposed approach as compared with others. The FRR value shows a significant decline of 5.4421, 5.7021 and 2.5611 while comparing with [27], [17] and [26]. Similarly, the FAR value shows a significant decline of 5.0671, 6.192 and 2.5611 while comparing with [27], [17] and [26]. In the current system, there are multiple ways to 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.

5. Conclusion

The proposed KNN-based machine learning technique has been successfully used to perform online verification using the dynamic parameters of the signature with greater

TABLE VIII. 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 Current Method	0.0579	0.0579	SVC2004

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. The objective of the proposed methodology is achieved on FRR and FAR value as shown in the result and discussion section. The minimized FRR and FAR value obtained in our proposed approach justifies it. The future exploration of the proposed work includes designing and developing the proposed and modified framework on the larger dataset.

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. Alaei, 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 combinational 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