MLP-Based Attribute Selection Method for Handwritten Signatures Authentication

Hemant A Wani[1], Kantilal Rane[2], V. M. Deshmukh[3]*

[1]Research Scholar, KBC NMU Jalgaon, Maharashtra, India
[2]Associate Professor, Bharati Vidhyapith College of Engineering, Navi Mumbai, Maharashtra, India
[3]Associate Professor, SSBT College of Engineering and Technology, Bambhori, Jalgaon, Maharashtra, India

Abstract. Finding the most unique traits that have strong discrimination capacities to be used for confirmation, in particular with reference to the substantial variation that's intrinsic in real signatures, is among the main difficulties in developing an algorithm for electronic signature validation. Handwritten signs offer the potential for expertly made frauds that closely resemble genuine equivalents. During this work, we proposed a methodical approach for authenticating online signs via an MLP that relies on a predetermined set of PCA (principal component analysis) features. This suggested method demonstrates an attribute selection methodology using data obtained from PCA calculations that is often disregarded but may be important in achieving a lower error rate. Utilizing a 5000-sign sample from the SIGMA database, the study produced false rates of acceptance (FAR) and false rates of rejection of 17.4% and 16.4%, respectively.

1 Introduction

Human biological features that may be utilized for identification are what is meant by the term "biometrics" [1]. Technologies for recognizing biometric data are often created for the purposes of identity and confirmation. The incorporation of biometric information in computerized systems for accessible monitoring and surveillance is increasingly pervasive in many open organizations, such as banking and ports [2]-[3]. A person's physical or behavioral characteristics may be utilized for modeling an authentication system [1]. Biological characteristics, including facial features, fingerprints, and eyes, are especially distinctive to each person and remain steady throughout time [1]. So, biometric devices that depend on these features are typically reliable and precise enough for recognition tasks involving one to many assessments [1]-[4]. However, behavioral characteristics like pronunciation, walking, and signatures can shift as time passes [1] and might be expertly imitated by a fake [5]. Consequently, creating a precise behavior-based biometric data system will be a difficult job. The handwriting sign is likely a particular biometric attribute that is widely recognized by everyone, although most biometric systems have security invasion problems [2]-[3].

* Corresponding author: *wanihemant1983@gmail.com*

This is mostly due to the long tradition of using signatures as proof of contractual and financial agreements [2]-[3]-[6]. All biological specimens of a person's signature that are obtained as part of an automatic handwriting authentication method are often kept in a file that serves as a standard pattern for use in later phases of validation. Nevertheless, among the biggest
problems with signature biometrics is intrauser variation, which is described as variations in a single user's authentic designs [7]-[10]. Additionally, if enough sign examples are available, a counterfeit may be created that closely resembles the authentic equivalents [8]-[11]-[12].
Onsite and offline techniques are both basic strategies for signature-driven biometrics [13]. The offsite method, often referred to as the stationary method, scans or photographs the handwritten signature once it has been written on paper using a webcam or scanner. While signing it, the web-based (dynamic) method, on the flip side, has the ability to gather flexible user traits (trajectories, pressure, speed, etc.) and convey the data via digitizing tools like a smartphone or touchscreen [13]. This study emphasizes the last strategy since it enables the collection of more detailed data besides the signature photographs.
A fundamental organizational layout of an online verification of signatures system is shown in Fig. 1 [16]. To be able to create a user's referencing model that is saved in the database, important information referred to as dynamic characteristics is first taken from sign examples during the registration step. The decision as to whether to grant or deny the requested signing samples as authentic or not is made after comparing them to the attributes of the newly inquired-about user using a template [17]. Due to intrauser variation, it is practically impossible for an individual to replicate their precise fingerprint on different tries. Intrauser variation quantifies the variance among a person's signature that can be impacted by difficulties with the surroundings, one's health, or one's emotions [14]-[18]. Numerous studies on both online and offline verification of signatures have been conducted in the last ten years without the express purpose of increasing confirmation efficiency [19]. Reduced computational complexity should be incorporated as well into the validation mechanism as possible to enable rapid reaction for applications in real-time [16]. The use of artificial neural network technology has been mentioned among other categorization approaches for robust verification applications [20]-[24]. As a result, we continue to employ ANN as a predictor in our research and concentrate on showcase-level improvements.
In order to accomplish that, they suggest using perform-based characteristics rather than traditional variable characteristics like the number of scribble-ups or scribble-downs and movement [16], which give more precise sign fluctuations. In order to simplify the information at hand, PCA is applied to the characteristic series of signals, such as line intensities and pen motions (x, y). First, PCA characteristics, including elements, latent, and score, are retrieved from time serial signals (x, y, and p). Then, to determine if the signature is real or fake, these characteristics are applied in the learning and validation phases of an MLP classification using an 8,000-item dataset of information and 200 participants.

2 Material And Methods

2.1 Collection of experimental handwritten signatures

One SIGMA dataset was utilized in this inquiry [25]. The 200 participants are divided into a random selection of twenty authentic, ten skill-forged, or ten non-skill-forged autographs per person. For every participant's signing samples in the learning stage, ten real, five non-skill-forged signings, and one skill-forged sign are selected. Likewise, the testing step uses the same number of specimens. A real signature has the number 1, whereas a fake one has the number 0. A total of 4,000 signature examples were chosen for the instructional set, while another 4,000 examples were utilized in the set of tests.

Table 1. Sampling Each for Evaluation And Instruction

Real signature	Samples of expertly fabricated signatures	Incompetently faked samples	Users in number	Total samples
20	10	10	200	8000

2.2 Methodology

PCA is used in this study to analyze the unique period information with the objective of condensing the space of attributes and finding novel, distinct characteristics. Then, using additional PCA calculation components like latent and score, we made a strategic choice of features. At the classification stage, the characteristics aggregated from the characteristics of features and selecting phases are used to form a signature.

Identification and Retrieval of Features One of the most commonly used statistical techniques for reducing dimensions, representing data, and extracting features in recognition of patterns and machine vision is PCA [26]. The fundamental idea behind PCA is to translate multiple circulations of data onto a smaller dimension with minimal loss of critical information. In order to do this, raw data with a strong correlation across variables is projected onto a new space. Prior to choosing features, we take into account six key processes for computing PCA in order to depict the feature set of each sign in reduced dimensions. The steps in the process are broken down as follows:

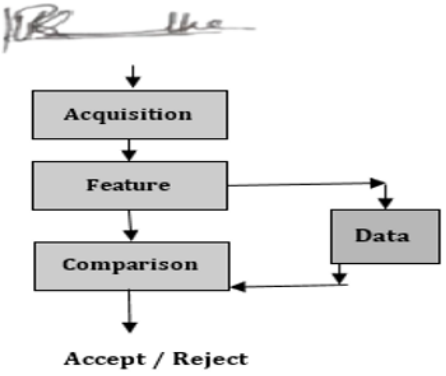


Fig. 1 Fundamental steps in PCA

1. Applying (1) to all of the variables (x, y, and p), get the dataset's average value as

$$\bar{X} = \frac{\sum_{i=1}^{n} X_i}{N} \qquad (1)$$

N stands for the quantity of accessible specimens.

2. To create a fresh matrix (data adjust) of Matlab identical dimensions, M(NxM), remove the average result (X) with every sampling value (X) as given in the calculation below:

$$\phi i = X_i - \underline{X} \qquad (2)$$

3: Find the relationship of every pair of components

$$Con(M) = \sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})/(N-1) \quad (3)$$

4: Use this formula to get the value of the eigen values resulting from the covariant:

$$|M - \lambda I| = 0 \quad (4)$$

5: Find the coefficients

$$|M - \lambda jI|ej = 0 \quad (5)$$

We give some information on the translation of several terms, including loaded to latent, eigen value to

6: With regard to the eigen values, keep the biggest eigen vector, K, as the major component. Score, and eigenvector to component, because we used a MATLAB workstation for our application. A vector called the latent describes each observation in the signature. To determine the score number in relation to each latent, we compute the projection error for each latent. The element in question is determined in the following manner and is a combination of the following components:

$$Component = Score \times Latent + Residual \quad (6)$$

Since the $x, y,$ and p parameters in our knowledge space are 3-dimensional in the environment, the result known as characteristics. By using these elements, we could reassemble the original data.
The term "residual" refers to data that cannot be completely clarified by all of the initial data's constituents. The amount of remaining data affects the total number of elements.

Thus, the initial characteristic of the information can be represented by one or more of the three resultant elements. The rating matrix's entries are arranged in descending order according to how much variation there is, which is also how the primary components are arranged. For example, as contrasted with the other two elements, the first element has the biggest variation value with regard to its score. The third element has the lowest variation value, whereas the following element contains the second-highest volatility.

2.3Verification

An MLP neural network that relies on the supervised learning approach of backpropagation serves as the classifier utilized in this study. An MLP neural network essentially consists of a layer for input, a layer that is concealed, and a layer for output. To get the intended result, these levels additionally interact via the network's characteristic vector movement and diffusion. Neural networks are computed using a set of source information, an input load at every neuron, and a certain bias. The result is a function based on the input's weighted average. This function, also known as an activation function, converts the value of the output amplitudes into a range of values.

2.4 Implementation For Systems & Performance Assessment

Iterative processes are used to train the network. To determine the layer that has hidden errors, the coefficients of weight (w) of neurons are modified at every iteration depending on the outcome defect that is sent through the layer that outputs to the front layer [27].

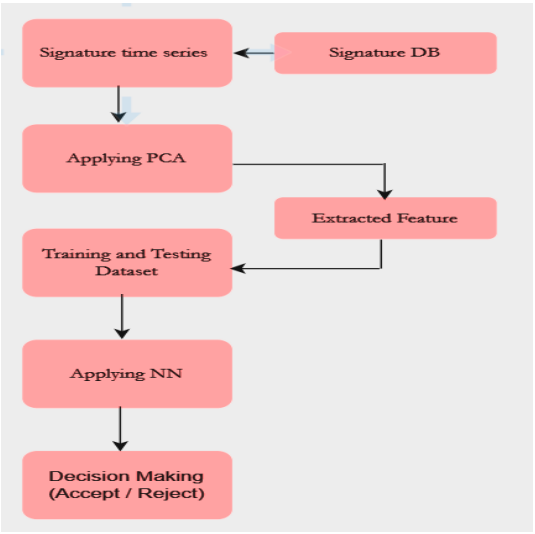
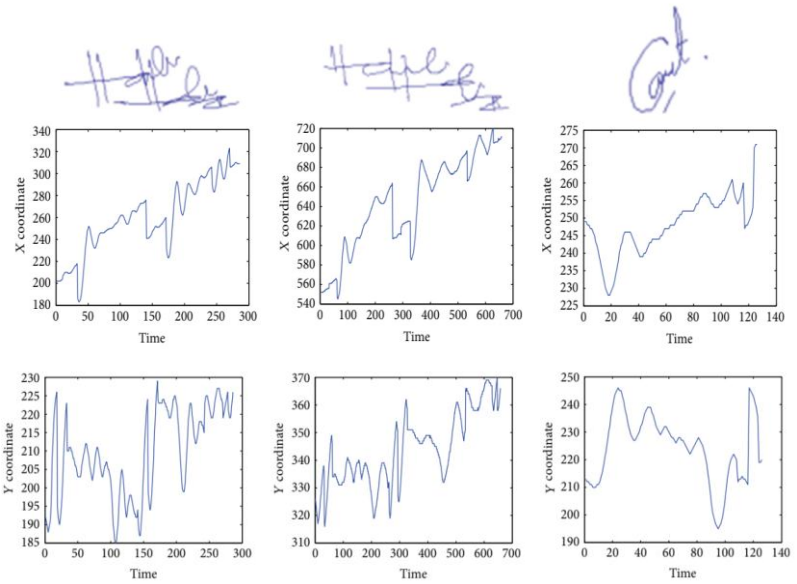


Fig. 2. A proposed online signature verification system's schematic design



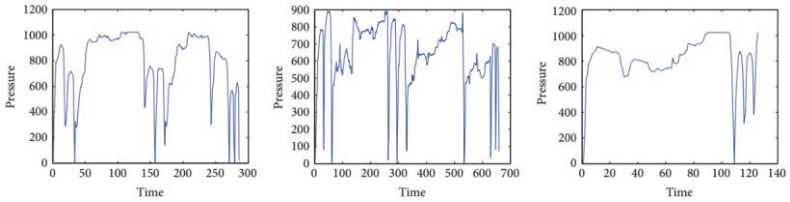


Fig. 3: a) genuine sign. ; b) skill-forged sign. and c) non-skill-forged sign collection are all shown in the SIGMA DB example of signing pens trajectory and pressure

Every neuron's response acts as a trigger for the next concealed level, and its weights (w) start out with low numbers that range from 0 to 1 [23]. In the section that follows, the formation procedure in a backpropagation.
The result (y), which is the linear sum of every input where i is the value that represents the input, l is the total value of the neurons, and N represents the total number of data samples [28], can be calculated as follows:

$$Y = \sum_{l=1}^{N} W_{il} X_l + W_{in+1} \quad (7)$$

The result (y) is subsequently contrasted with the expected outcome to find e. The next equation illustrates the deviation in outcome.

$$E = \frac{1}{2} \sum_{l=1}^{N} (tl - ol)^2 \quad (8)$$

The error comes down to determining the incorrect value (δ) of every layer (for instance, layer j):

$$\delta j = oj(1 - oj) \sum_k W_{kj} \delta_k \quad (9)$$

The variance for every neuron is utilized to modify the neuron's parameters so as to decrease the total amount of error while offering a final result:

$$w_{ij}^{k+1} = w_{ij} + \eta \delta_j o_i \quad (10)$$

2.5 Training

A method has to acquire an illustration of the knowledge set throughout training that produces the least amount of generalization errors. The acquiring distortion might be decreased by average signatures over the bending route since DPM allows connections between multiple signatures. The average signing is additionally a more reliable way to represent the category. The mean signatures might be calculated when a training set contains a maximum of three instances if there is correspondence between all of the instances; nevertheless, this kind of relationship is difficult to construct. The comparison of all the cases may theoretically be done simultaneously using an N-dimensional vector rather than a matrix of values.

Also, provide a less-than-ideal training method: To discover all pairs' mean signatures from the set used for training, we solely use pair comparison. Finally, an example averaged signature is chosen, which yields the smallest alignment expense for the average sign for the remaining set of training signals. The model representing the initial set is calculated as the

median of all the matched signatures, and consistency among every one of the signatures included in the training set is acquired by aligning the signature using the original sign.

In this case, we may have multiple examples of one identity that correlate with a single instance of the reference signature, and vice versa if the distorted route supplied by DPM is noninvertible. The average of everything at the indicated locations yields a matching sample for the test, and the usual departure of each sample is afterwards utilized for calculating a weighted connection determined among signatures. All data values for every sign in the trained dataset that correspond to a specific example from the referring sign are used to create the models. A number of examples of signatures, training designs, and related skillful forgeries are displayed.

The training collection's sign match procedure's neighborhood data are summarized by the initial version and the local variance. To calculate the general alignment procedure, each of the leftover differences between the initial set's signature and the final product are gathered. To use the distances as normalizing parameters for categorization, we take the mean and the mean relative variation of these values. These ranges are also used to establish the refusal limit for the experiment's outdoor testing. Users can choose the cutoff value, which is equivalent to the average plus five situations of the average variation of the distances.

2.6 Testing

The signature validation method may be verified using various fakes based on the information that is available. The two most frequent forgery kinds are randomized forgeries, in which the counterfeiter uses his own handwriting as the sign to be validated, and skill forgeries, in which the forger attempts and practices replicating the dynamic and static data of the actual sign as nearly as possible. In the tests outlined in paragraph 5, we utilized both sorts of fraud. The verifiable effectiveness of the method was assessed for both all of the information collections and each participant separately. Neither random nor expert forgery produced erroneous compromise charts.

The graphs for competent forgery with the actual test error rates were calculated using the test set and fakes set for every topic; the graphs for randomized forgery were obtained using the testing set along with every one of the other respondents' signatures. The efficacy of the system's identification was assessed using the test sets.

The length of the signature was used to hurry up the trials and weed out obvious frauds. From the instruction set, the average length of each subject's signature was taken. The time length of each signature that was being tested was examined to ensure that it fell within three percentage points of the typical length for the relevant participant. Signatures that fell within these parameters were compared to the prototypes via DPM, whereas those that were beyond them were eliminated as frauds. This broad screen failed to result in any erroneous rejections but decreased the number of DPM matches to be made by around 40%.

2.7 Error Rates

Verification: The collection of genuine signatures and the class of fraudulent signatures are the two classes that make up the structure of the recognition problem of confirming a sign. The efficacy of the verification method is often evaluated using Type I and Type II error rates. The type I error rate, also referred to as the FRR, is an indicator of the proportion of validated signatures that are forgeries as a result of being classified for classification.

The number of counterfeit identities that are accepted as legitimate ones is measured using the Type II error percentage, also known as the fake acceptance ratio (FAR). The error rate trade-off graph shows the relationship between FAR and FRR using the categorization level as a variable. The equivalent rate of error, meaning the error rate when the proportion of

erroneous acceptances equals the proportion of false rejections, is a practical way of summarizing this curve. The method's statistical efficiency, or more specifically, its generalization error, is estimated by the same rate of error. The usual curves of FRR and FAR as functions of the category criterion and the associated error compromise curve are shown in Fig. 3.

A real field test, meaning a test that simulates the setting up and operation of the system's components in an actual setting, offers a distinct characterization of the verified functionality of the system as a whole.

2.8 Signature Recognition

The M-class pattern identification issue of recognizing signatures requires the algorithm to choose the category to which a particular identity belongs. Given that the computer system cannot predict beforehand the purported class of case in question, recognizing a signature is a more challenging task than confirming a signature. The metric used to assess the system's effectiveness in terms of recognizing signs is the identification error percentage, which counts the number of incorrectly categorized signatures. Outcomes for recognizing signatures are displayed on the subject's experiment.

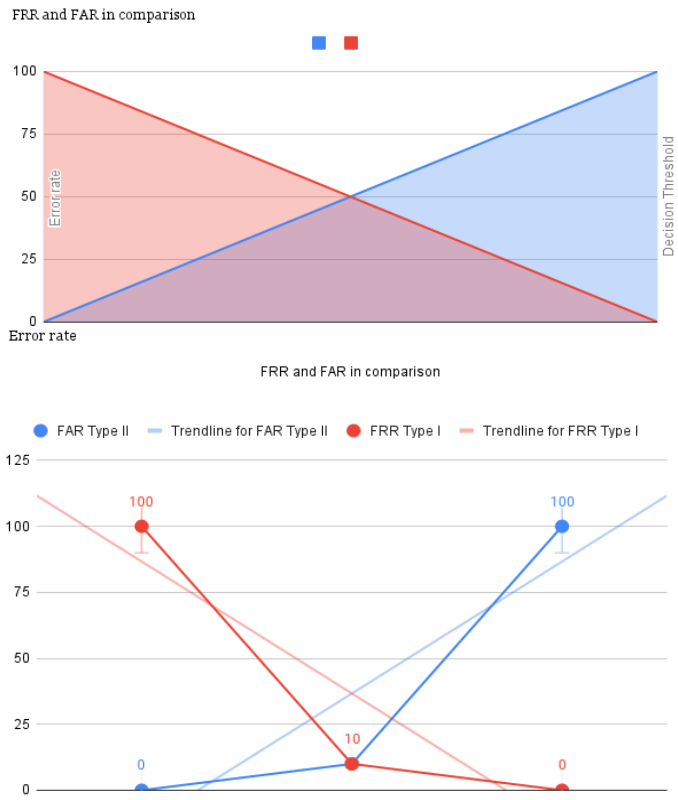


Fig. 4 a. FRR and FAR in comparison b. Errors compromise curves.

a) FRR and FAR in comparison to the categorization criterion It is obvious that we may substitute one form of error with another type of error. Accepting all signatures indicates a 0% FRR and 100% FAR, whereas rejecting all signatures means a 100% FRR and 0% FAR.

(b) Errors compromise curves.

It gives the method's behavior for each OS and is the most accurate way to describe the computer's efficiency.

If one can conduct the execution of the study in a constrained context, we can conduct the assessment of a model by providing empirical data. This is done to assess if the outcomes meet our specified standards, such as being practicable and trustworthy, etc. The investigator is going to be able to determine when the precision meets the intended precision by putting it into effect under controlled settings and seeing when it is successful. In the case of machine learning, a model is evaluated using primarily two techniques. They are cross-evaluation and hold-out strategies. Both of these methods use a test set to prevent issues brought on by excessive fitting.

The hold-out approach is applied to big databases as a whole and is composed of three components: a training set, the set for validation, and the test data collection.

The k-fold cross-evaluation approach, however, focuses mainly on datasets that are somewhat smaller in size. We chose the k-fold cross-evaluation approach because our data set only contains a small quantity of information. In this case, the dataset is divided into k subsets, each of which has the same size.

It uses a five-step cross-validation approach for the study being suggested. Several approaches are used to carry out the execution. First, the whole set is split into five identical subsets, each of which has the same amount of information. Among the five, one is chosen to serve as a test set, while the others are used to train the design. Once the command is evaluated, multiple calculations depending on various factors, like false-positive, true-negative, true-positive, and false-negative, occur. Following that, the data from both the examination set and the practice set are computed, and the outcomes are averaged. The learning model will use a piece of the information during the test phase.

First, determine the information's correctness, and then compute all four different variables. They are listed above in the following order:

$$Precision = TP\ x\ (1/\ TP + FN)$$

Remember, this value is the anticipated favorable result of all beneficial characteristics.

$$Recall = TP\ x\ (1\ /\ (TP + FN))$$

The F1-Score is determined by averaging the accuracy and Retention scores

$$F1\ score\ is\ calculated\ as\ 2 * [\ (precision + recall)\ /\ (Precision + Recall)]$$

3. Experimental Result

For each user in our study, we used five expertly fabricated signature samples and 10 real signature samples. Additionally, we included five additional real signature samples from a person who was chosen at random to have non-skillfully fabricated signatures. The verification matrix is created by combining ten further real signature samples from the same user, five skill-forged signature samples from that user, and five genuine signature samples.

Here, as remarked, the choice of the principal components is very heuristic in order to get a reliable identification rate. As a result, we first used all three of the accomplished components as features. As a result, the feature vector used to represent a signature sample is made up of just nine values as opposed to the high-dimension space. The recognition rate

of just 82% suggests that these nine variables are insufficient to create a trustworthy online signature verification system.
The outcomes of the test are shown in Table 2, where the suggested method is able to obtain 95.1% accuracy and FAR and FRR of 17.4% and 16.4%, respectively.

Table 2. Sampling Each for Evaluation And Instruction

Accuracy (%)	**FAR (%)**	**FRR (%)**
95.1	17.4	16.4

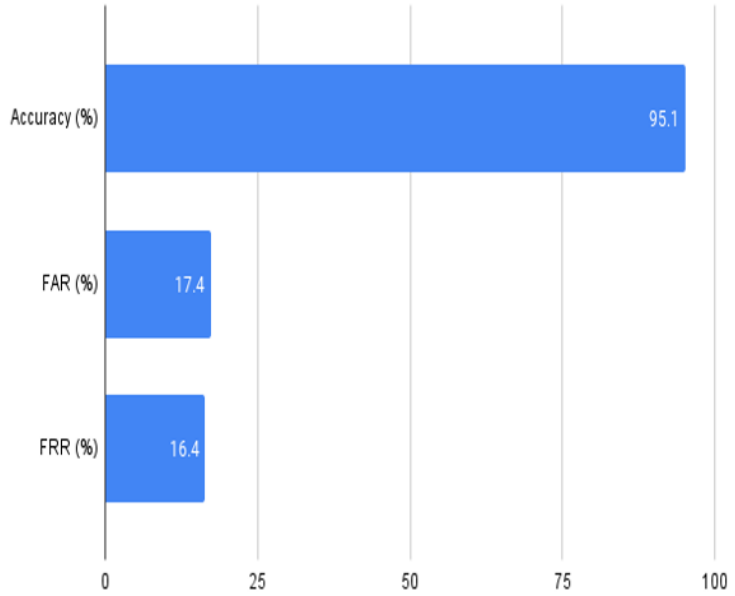


Fig. 5. Bar represents the Error Rate of identification

Table 3: Several similar SIGMA database implementations

Reference No.	**Classifier**	**Feature extraction**	**No. of obtained features**	**No. of samples in training**	**No. of samples in testing**	**FAR (%)**	**FRR (%)**	**Accuracy rate (%)**	**Threshold value**
14	ANN	Pearson Correlation	19	4000	4000	31.3	23.8	84.4	NA
16	ANN	PCA	172	4000	4000	18.5	34.3	85.5	NA
Proposed	ANN	PCA	60	4000	4000	17.4	16.4	95.1	0.6

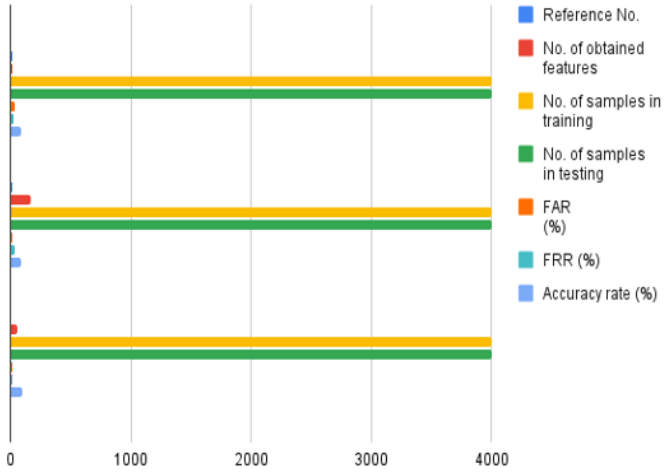


Fig. 6. Bar represents the comparative Analysis of different classifiers with the Proposed System

Table 3 compares prior methods on the SIGMA database in order to better understand the impact of the chosen features from PCA analysis on recognition outcomes. Table 3 clearly shows that the suggested method outperformed the approaches described in [14, 15], despite utilizing a comparable classifier (ANN), the identical number of examples for testing and training, and distinct attribute identification and extraction procedures.

4 Conclusion and mathematics

This paper proposes a unique technique for selecting traits for the validation and recognition of handwritten electronic signs. As suggested, extract 50 important characteristics from Sigma handwritten signatures using PCA to represent each unique signature. After that, an MLP is used to determine whether the signatures are fake or real. The verification result, which included both expertly faked and real signs, shows the value of the recommended strategy, as it obtained 95.1% accuracy for 200 participants with 8,000 signs.

References

1. Singh, N., Kumar, M., Singh, B. et al. DeepSpacy-NER: an efficient deep learning model for named entity recognition for Punjabi language. Evolving Systems 14, 673–683 (2023). https://doi.org/10.1007/s12530-022-09453-1
2. A. Mehmood, “Brain tumor localization and segmentation using mask RCNN,” Frontiers of Computer Science, vol. 15, no. 6, article 156338, 2021.
3. M. Kumar, “Recognition of offline handwritten Urdu characters using RNN and LSTM models,” Multimedia Tools and Applications, vol. 82, no. 2, pp. 2053–2076, 2023.
4. Y. M. Al-Omari, S. N. H. S. Abdullah and K. Omar, "State-of-the-art in offline signature verification system," 2011 International Conference on Pattern Analysis and Intelligence Robotics, Kuala Lumpur, Malaysia, 2011, pp. 59-64, doi: 10.1109/ICPAIR.2011.5976912.

5. S. N. Yanushkevich,et al. "Synthetic biometrics: a survey," in Proceedings of the International Joint Conference on Neural Networks (IJCNN '06), pp. 676–683, Vancouver, Canada, July 2006.
6. A. A. Ross, et al. Handbook of Biometrics, Springer, 2008.
7. A. Nagar,et al. "Biometric template security," EURASIP Journal on Advances in Signal Processing, vol. 2008, Article ID 579416, 2008.
8. S. Albahli, T. Nazir, A. Irtaza, and A. Javed, "Recognition and detection of diabetic retinopathy using DenseNet-65 based faster-RCNN," Computers, Materials and Continua, vol. 67, no. 2, pp. 1333–1351, 2021.
9. M. Nawaz, M. Masood, A. Javed et al., "Melanoma localization and classification through faster region-based convolutional neural networks and SVM, " Multimedia Tools and Applications, vol. 80, no. 19, pp. 28953–28974, 2021.
10. M. Nawaz, T. Nazir, A. Javed et al.,"An efficient deep learning approach to automatic glaucoma detection using optic disc and optic cup localization, " Sensors, vol. 22, no. 2, p. 434, 2022.
11. S. Pashine, R. Dixit, and R. Kushwah, "Handwritten digit recognition using machine and deep learning algorithms," 2021, http://arxiv.org/abs/2106.12614.
12. V. Athila and A. S. Chandran, "Comparative analysis of algorithms used in handwritten digit recognition," International Research Journal of Engineering and Technology, vol. 8, no. 6,2021.
13. H. H. Zhao and H. Liu, "Multiple classifiers fusion and CNN feature extraction for handwritten digits recognition," Granular Computing, vol. 5, no. 3, pp. 411–418, 2020.
14. E. A. Enriquez, N. Gordillo, L. M. Bergasa, E. Romera, and C. G. Huélamo, "Convolutional neural network vs traditional methods for offline recognition of handwritten digits," in Advances in Physical Agents. WAF 2018. Advances in Intelligent Systems and Computing, vol 855, R. Fuentetaja Pizán, Á. García Olaya, M. Sesmero Lorente, J. Iglesias Martínez, and A. Ledezma Espino, Eds., Springer, Cham, 2019.
15. D. Y. Ge, X. F. Yao, W. J. Xiang, X. J. Wen, and E. C. Liu, "Design of high accuracy detector for MNIST handwritten digit recognition based on convolutional neural network," in 2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA), pp. 658 –662, Xiangtan, China, 2019.
16. A. Beikmohammadi and N. Zahabi, "A hierarchical method for Kannada-MNIST classification based on convolutional neural networks, " in 2021 26th International Computer Conference, Computer Society of Iran (CSICC), pp. 1–6, Tehran, Iran, 2021.
17. A. K. Agrawal, "Design of CNN based model for handwritten digit recognition using different optimizer techniques, " Turkish Journal of Computer Mathematics Education, vol. 12, no. 12, pp. 3812 –3819, 2021.
18. W. S. Wijesoma, K. W. Yue, K. L. Chien, and T. K. Chow, "Online handwritten signature verification for electronic commerce over the internet," in Web Intelligence: Research and Development, vol. 2198 of Lecture Notes in Computer Science, pp. 227–236, Springer, 2001.
19. S. Nanavati, M. Thieme, and R. Nanavati, "Other leading behavioral biometrics," in Biometrics: Identity Verification in a Networked World, chapter 9, pp. 123–131, John Wiley & Sons, New York, NY, USA, 2002.
20. Y. M. Al-Omari, S. N. H. S. Abdullah, and K. Omar, "State-of-the-art in offline signature verification system," in Proceedings of the International Conference on Pattern Analysis and Intelligent Robotics (ICPAIR '11), vol. 1, pp. 59–64, June 2011.

21. S. N. Yanushkevich, "Synthetic biometrics: a survey," in Proceedings of the International Joint Conference on Neural Networks (IJCNN '06), pp. 676–683, Vancouver, Canada, July 2006.
22. A. K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics, Springer, 2008.
23. K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," EURASIP Journal on Advances in Signal Processing, vol. 2008, Article ID 579416, 2008.
24. E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," IEEE Transactions on Systems, Man, and Cybernetics A: Systems and Humans, vol. 40, no. 3, pp. 525–538, 2010.
25. E. A. Rua, E. Maiorana, J. L. A. Castro, and P. Campisi, "Biometric template protection using universal background models: An application to online signature," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 269–282, 2012.
26. E. Grosso, L. Pulina, and M. Tistarelli, "Modeling biometric template update with ant colony optimization," in Proceedings of the 5th IAPR International Conference on Biometrics (ICB '12), pp. 506–511, New Delhi, India, April 2012.
27. F. H. Alvarez and L. H. Encinas, "Security efficiency analysis of a biometric fuzzy extractor for iris templates," in Computational Intelligence in Security for Information Systems, vol. 63 of Advances in Intelligent and Soft Computing, pp. 163–170, Springer, Berlin, Germany, 2009.
28. A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in Media Forensics and Security II, 75410, vol. 7541 of Proceedings of SPIE, San Jose, Calif, USA, January 2010.
29. S. Rashidi, A. Fallah, and F. Towhidkhah, "Feature extraction based DCT on dynamic signature verification," Scientia Iranica, vol. 19, no. 6, pp. 1810–1819, 2012.
30. I. A. Ismail, T. El danf, M. A. Ramadan, and A. H. Samak, "Automatic signature recognition and verification using principal components analysis," in Proceedings of the 5th International Conference on Computer Graphics, Imaging and Visualisation, Modern Techniques and Applications (CGIV '08), pp. 356–361, IEEE, Penang, Malaysia, August 2008.
31. N. Xu, Y. Guo, L. Cheng, X. Wu, and J. Zhao, "A method for online signature verification based on neural network," in Proceedings of the IEEE 3rd International Conference on Communication Software and Networks (ICCSN '11), pp. 357– 360, Xi'an, China, May 2011.
32. A. U. Khan, T. K. Bandopadhyaya, and S. Sharma, "Comparisons of stock rates prediction accuracy using different technical indicators with backpropagation neural network and genetic algorithm based backpropagation neural network," inProceedings of the 1st International Conference on Emerging Trends in Engineering and Technology (ICETET '08), pp. 575–580, July 2008.
33. A. H. Monahan, "Nonlinear principal component analysis by neural networks: theory and application to the Lorenz system," Journal of Climate, vol. 13, no. 4, pp. 821–835, 2000.
34. S. M. S. Ahmad, A. Shakil, A. R. Ahmad, M. A. Muhamad, and R. M. Anwar, "SIGMA—a Malaysian signature's database," in Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, pp. 919–920, March 2008.

35. M. Suganthy and P. Ramamoorthy, "Principal component analysis based feature extraction, morphological edge detection and localization for fast iris recognition," Journal of Computer Science, vol. 8, no. 9, pp. 1428–1433, 2012.
36. N. Xu, L. Cheng, Y. Guo, X. Wu, and J. Zhao, "A method for online signature verification based on neural network," in Proceedings of the IEEE 3rd International Conference on Communication Software and Networks (ICCSN '11), pp. 357– 360, Xi'an, China, May 2011.
37. A. Shukla, J. Dhar, C. Prakash, D. Sharma, R. K. Anand, and S. Sharma, "Intelligent biometric system using PCA and R-LDA," in Proceedings of the WRI Global Congress on Intelligent Systems (GCIS '09), vol. 1, pp. 267–272, Xiamen, China, May 2009.