International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 12, December 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Online Signature Verification Using Recurrent Neural Network

Hemant A. Wani, Divya P. Surwade, Kantilal Rane, V.M.Deshmukh

1. Research Scholar, KBC NMU Jalgaon, Maharashtra, India

2. Assistant Professor, KCE'S College of Engineering and Management, Jalgaon

3. Assosiate Professor, Bharati Vidhyapith College of Engineering, Navi Mumbai, Maharashtra, India

4. Assosiate Professor, SSBT College of Engineering and Technology, Bambhori, Jalgaon, Maharashtra, India

Abstract

Using biological traits of humans to identify them, biometrics has grown more and more common in many identification systems. Online signature-based biometrics, which record dynamic user attributes including trajectories, pressure, and velocity, are the specific focus of this work. The goal of the project is to enhance online signature verification systems' effectiveness by utilizing function-based characteristics and simplifying the data through Principal Component Analysis (PCA). The classifier is an artificial neural network (ANN). The SIGMA database, which contains 200 users' authentic, skill-forged, and non-skill-forged signatures, is used for the evaluation. The suggested strategy yields low rates of false acceptance and rejection, with a recognition accuracy of 93.1%, according to the results. The study comes to the conclusion that other elements, such latent and score values, affect accuracy of the verification system, indicating how well the recommended feature selection technique works for recognizing online signatures.

Keywords: Artificial Neural Network (ANN), Principal Component Analysis (PCA), dynamic user attributes, feature level improvement, biometrics, and online signature verification.

INTRODUCTION

The use of a person's biological traits for identification is known as biometrics [1]. Online and offline techniques are the two main approaches for signature-based biometrics [10]. The offline approach, sometimes referred to as the static method, uses a camera or scanner to scan or take a picture of the signature after it has been written on paper. By using digitizing instruments like a tablet or touchpad, the online (dynamic) technique—the subject of this study—extracts dynamic user variables including trajectories, pressure, and velocity during the signature process [13]. With this method, more comprehensive data, including signature photos, can be gathered.

Figure 1 illustrates the basic structure of an online signature verification system [15]. In the registration phase, relevant information, i.e., dynamic features, are extracted from the signature samples to create a user and reference model, which are then stored in the database. When sending a new signature sample, the system compares it with the stored template to make a decision about its authenticity [11]. Reproducing an exact signature across multiple companies is difficult for users due to the variability of intruders. This variation measures the differences between a person and their signatures, which are influenced by, for example, environmental conditions, health or emotional state [14].

Over the past decade, many studies have been conducted on online and offline signature verification, with the clear goal of improving verification accuracy [8]. At the same time, there is a recognized need to minimize the complexity of data processing in control systems to ensure fast response in real-time applications [13]. Among the various classification

methods for strong authentication, the Artificial Neural Network (ANN) technology has emerged as an outstanding choice. Therefore, in this paper, we continue to use ANN as a classifier and focus on improving the feature level.

To achieve this, we recommend using feature-based functions instead of traditional parameter functions such as pen up and down and number of strokes [15]. Action-based features describe the signature dynamics more precisely. Principal component analysis (PCA) is applied to the characteristic time series signals, including pen pressure and trajectory (x, y), to smooth the dataset. Initially, PCA features including components, latent variables and prices are derived from the time series signals (x, y, p). Later, these features are used in the training and testing phase of a multilayer perceptron (MLP) classifier using a dataset of 200 users and 8000 samples to detect signature authenticity by distinguishing between genuine and forged signatures.

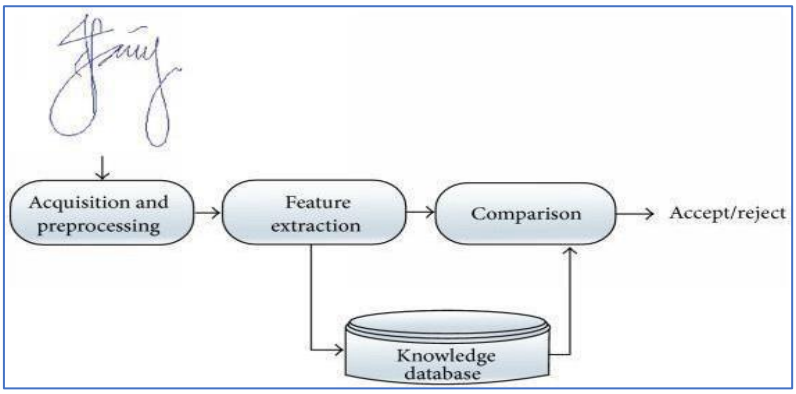


Fig:1. Online signature verification system scheme.

RELATED WORKS

Signature verification is a form of biometric authentication that plays a key role in many areas, including administrative and legal applications, where user authentication is essential. Its importance extends to banking systems, where individual signatures act as unique identifiers, similar to fingerprints. Distinctiveness of signatures is crucial in determining the legal owner or approval of an official document. Despite an individual's inherent uniqueness and signature style, the possibility of imitation exists through repeated attempts. Machine learning and deep learning techniques have been used to mitigate this threat and effectively distinguish between genuine and forged signatures. These advanced technologies improve signature verification systems and provide a stronger and more reliable authentication method.

In the study presented in [3], the authors propose a time-based recurrent neural network (RNN) as a solution to the online signature verification problem. Their innovative methods include the integration of dynamic time warping into an RNN network, resulting in powerful models designed to effectively discriminate between forged signatures. This approach reflects a strategic combination of methods to improve the overall performance of the authentication system. In contrast, in [4], a frame-independent architecture based on a convolutional neural network is introduced in the signature verification process. Their sCNN (Shallow Convolution Neural Network) architecture consists of three convolutional layers and one fully connected layer. In particular, their trained model stands out for its simplicity in terms of the number of core layers, which stands out from more complex methods. This deliberate simplification results in the optimization of a reduced number of weight parameters, which ultimately streamlines the training and testing processes. The authors claim that the sCNN model shows better results in terms of accuracy and error rate compared to alternative methods.

In work [5], they used a Convolution Neural Network as a sub-network to develop an application based on offline signature verification, creating a Siamese network In a Siamese network, they plan to make the discrimination of real forged signatures more accurate by adding some statistics. properties to the input vector, which is a mathematical expression of each signature image. Research [6] showed that RNN can be used to solve the problem of online signature verification. They used a model designed to authenticate network signatures by combining RNN LSTM and Siamese network. By measuring the similarity between two signature samples, they allowed the model to learn this.

DATABASE AND PROCESSING

The study used the SIGMA database containing 200 users randomly divided into subsets containing 20 authentic, 10 clever forged signatures for each user. In the training phase, each user and signature sample is submitted by selecting 10 genuine, 5 skill forged and 5 non-skill forged signatures. This distribution is mirrored in the testing phase so that sample sizes remain consistent. Authentic signatures are given the identifier and#039;1 and#039; while forged is marked and#039;0.and#039; A total of 4000 signature samples were selected for the training set and another 4000 signature samples for the test set. In the database mentioned below, the signatures are represented as time series signals at each sample point, such as pen pressure (p) and trajectory (x, y) in Figure 2. As initially stated in Section 3, for our selected subset of signatures. , each signature sample in the SIGMA database consists of three time series signals (x, y, p), resulting in a high-dimensional feature vector. To represent each signature in the lower dimension of the feature space, we consider six basic steps to compute PCA. Represent each signature in the lower dimension of the feature space before selecting a feature. The procedural steps are simplified as follows.

Step 1: Find the mean value of dataset X using (1)on each variable (x, y, p):

Where N is the number of available samples

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

Where N is the number of available samples.

Step 2: Subtract the mean value (X)from each

sample value (X) as shown in the following equation to have a new matrix (data adjust) with the same dimension, M(N*M) : $\emptyset i = Xi - \bar{X}$ **(2)**

Step 3: Compute the covariance of any two variables, (x, y), (x, p), and (y, p), separately using (3) on the previous matrix (N*M) :

$$Cov(M) = \frac{\sum_{i=1}^{n}(Xi-\bar{X}(Yi-\bar{Y})}{(N-1)} \quad (3)$$

Step 4: compute the eigenvalues from covariance matrix by Using the following equation,:

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

Step 5: Also, calculate the eigenvectors from the covariance matrix using the following equation : : $(M - \lambda jI)ej = 0$ (5)

International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 12, December 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Step 6: Finally, retain the largest eigenvectors K as the principal components with respect to the eigenvalues.

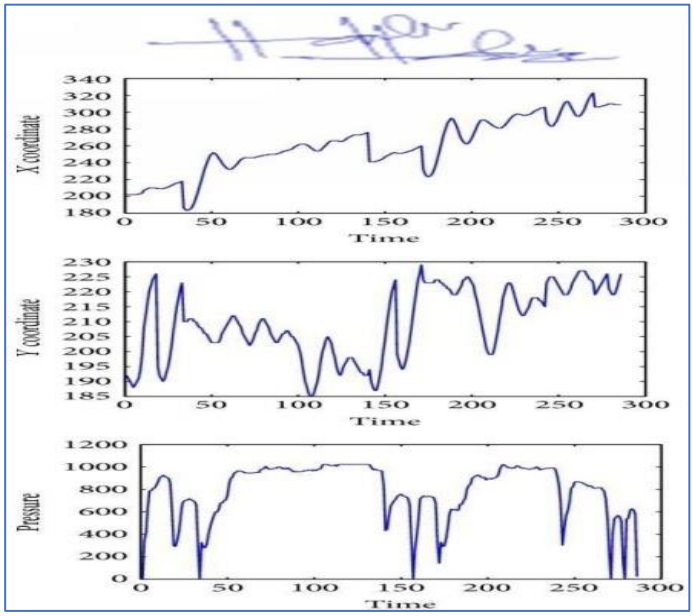
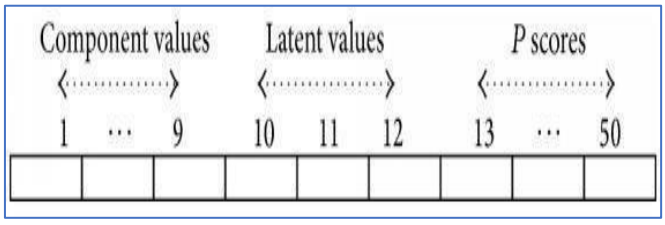


Fig:2. Signature Sample in the SIGMA Database

We provide information on converting some terms, such as charge to latent, eigenvalue to point, and eigenvector to component. Therefore, we used MATLAB workstation in our implementation. Latency is a vector that describes all the observations in a signature. For each latent value, we also calculate the projection error to obtain a score relative to that latent. to get a score for latency, we calculate the projection error. Finally, a given component is a combination of three elements and is calculated as follows:

$$component = score \times latent + residual \quad (6)$$

The first component is selected in addition to the nine features used in the previous experiment. 38 scores from the entire scoring matrix were also used. Therefore, 50 salient features, which are combinations of the nine component features, formed the resulting feature representation for each signature. Figure 4 shows values, three hidden values and 38 points. Specifically, each latent value score is determined by estimating the projection error. The resulting component is a combination of three elements, which is calculated according to the following formula (6). In this calculation, the first component containing the nine properties used in the previous experiment is selected. Also included are 38 scores taken from the entire scoring matrix. Thus, each signature feature representation contains 50 salient features composed of nine component features. Figure 4 presents these values visually, including three hidden values and 38 points.



International Journal of Advance Research in Science and Engineering
Volume No. 12, Issue No. 12, December 2023
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Fig:3. three-dimensional space Component

The result of the PCA transformation of the data consists of three components that act as features due to the three-dimensional space inherent in the data set and #039, including the variables (x, y) and (p). These components can be used to restore the original data. In this context, the residue refers to the information in the original information that is ignored by the components. Determining the number of components depends on the amount of residual information in the initial knowledge.

RESULT AND DISCUSSION

In this study, we included five expertly forged signature samples and ten authentic signature samples for each user. In addition, we presented five genuine signature samples from a randomly selected user (user 193), which included unqualified fake signatures. Therefore, in the testing phase, we combined ten authentic signature samples of the same user, five authentic signature samples of user 193, and five cleverly forged signature samples of this user to form the test matrix. Thus, unlike a high-dimensional space, the feature vector used to represent a signature sample contains only nine values. However, the detection rate of only 82% suggests that these nine variables are not sufficient to create a reliable signature verification network. This result highlights the need for more comprehensive features to improve system performance and reliability.

Then, as described in Section 3, we investigated the proposed PCA feature selection technique, which includes additional information such as latent and score. The first latent vector in Figure 4. Vector representing the user's signature. system But because each signature and length is different from the next, we chose a random score from the score matrix instead of the first 38, because each score The test results are shown in the table, where the proposed method achieved 93.1% accuracy and false. Acceptance rates (FAR) and false rejection (FRR) are 7.4% and 6.4%.

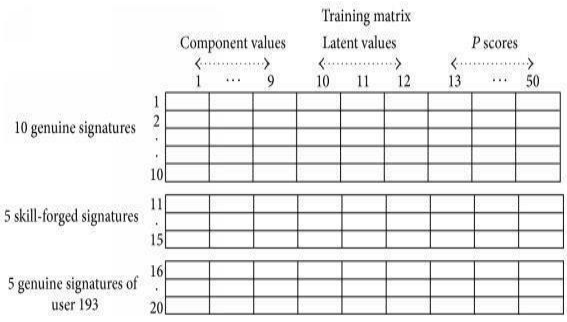


Fig:4. Sample of training and testing matrices per user.

$$Accuracy(\%) = 100(\%) - \left[\frac{(FRR+FAR)}{2}\right] \qquad (7)$$

Accuracy (%)	FAR (%)	FRR (%)
93.1	7.4	6.4

Table: Recognition and error rates.

After using principal component analysis (PCA) to represent signatures in the verification system, the performance of the proposed online signature verification (OSV) system in this study was evaluated using 50 features. The evaluation used a dataset of 200 users and 8,000 signature samples, resulting in a commendable recognition accuracy of 93.1%. In particular, it became clear that using fewer signature features during training produced results characterized by lower validity, higher false acceptance rate (FAR) and false rejection rate (FRR), and decreased overall accuracy.

In addition, the experiment and results emphasize that adding additional components such as latent and score values to PCA-derived features, which have been widely used in previous studies, contributes to high accuracy. The achieved FRR and FAR values were approximately the same as reported in Table 4. This almost identical difference indicates a comparable error rate in distinguishing between genuine and forged signatures. Thus, the average FAR and FRR values calculated at 6.9% can be interpreted as a misclassification rate close to the equal error rate (EER). It is worth noting that the signature sample and length calculated from the point element are understandable for 38 pen trajectories and pressure samples. Meanwhile, the minimum signature length of this study exceeded 100 observations.

CONCLUSION

The methodology proposed in this study centres on feature selection for the verification and identification of digital handwritten signatures. To achieve this objective, we extracted 50 key features from Malaysian handwritten signatures using Principal Component Analysis (PCA), providing an efficient representation for each distinct signature. Subsequently, a Multilayer Perception (MLP) model was employed for the classification task to discern whether the signatures were genuine or fake. The MLP model underwent training utilizing a dataset comprising 200 users and 8,000 signatures, encompassing both skills fully crafted fake signatures and authentic ones. The outcomes of the verification process underscore the effectiveness of the suggested method, yielding an accuracy rate of 93.1%. This outcome indicates that the proposed feature selection technique, when coupled with the MLP classifier, proves highly proficient in distinguishing between counterfeit and authentic signature.

235

REFERENCES

1. A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125– 143, 2006.

2. 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.

3. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Ortega-Garcia, J. (2021). DeepSign: Deep On-Line Signature

4. Jain, A., Singh, S.K., Singh, K.P. (2020). Handwritten signature verification using shallow convolutional

5. Jagtap A.B., Sawat D.D., Hegadi R.S., Hegadi R.S. (2019). Siamese Network for Learning

Genuine and Forged.

6. Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Ortega-Garcia, J. (2017). Biometric Signature

Verification Using Recurrent Neural Networks. In: 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), pp. 652-657. Kyoto, Japanpp. 131-139.A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*, Springer, 2008.

7. K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 579416, 2008.

8. 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.

9. 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.

10. 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.

11. F. H. Álvarez 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.

12. 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.

13. S. Rashidi, A. Fallah, and F. Towhidkhah, "Feature extraction based DCT on dynamic signature verification," *ScientiaIranica*, vol. 19, no. 6, pp. 1810–1819, 2012.

14. V. Iranmanesh, S. M. S Ahmad, W. A. W. Adnan, F. L. Malallah, and S. Yussof, "Online signature verification using neural network and pearson correlation features," in *Proceedings of the IEEE Conference on Open Systems*, pp. 18– 21, 2014.

16. F. L. Malallah, S. M. S. Ahmad, W. A. W. Ahmad, V. Iranmanesh, and S. Yussof, "Online signature temple protection by shuffling and one time pad schemes with neural network verification," in *Proceedings of the*

International Conference on Computer Science and Computational Mathematics (ICCSCM '13).

17. Hemant A. Wani, Kantilal Rane, V. M. Deshamukh, "MLP–Based Attribute Selection Method for Handwritten Signature Authentication *" in ITM Web of Conferences 57, 01017(2023) ICAECT* 2023.

18. Vahab Iranmanesh, Sharifah Mumtazah Syed Ahmad, Wan Azizun Wan Adnan, Salman Yussof et al. "Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis", *The Scientific World Journal*, 2014.