A Comprehensive Study on Offline Signature Verification

Neha Sharma¹; Shefali Gupta¹* and Puneet Mehta²

¹Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India
²Chandigarh Group of Colleges – College of Engineering Landran, Punjab India

Corresponding Author : Shefali Gupta. Email: shefali.gupta@chitkara.edu.in

Abstract: Handwritten Signatures are special types of behavioural biometric which are used in many applications such as banks, credit cards, passport, check processing, and financial documentation, etc. Verification of these signatures is a challenging task especially in the case of offline where there is no information of signing process. So there is a need for a system that can distinguish between the genuine and the forged signature to avoid the chances of theft or fraud. Many types of researches have been done in this area in the last three decades. Earlier this task was performed by handcrafted features and recently deep learning techniques have been employed for this task, but still, there is a chance of enhancement in the accuracy of the system. In this paper, we present a comprehensive study of the work done in the field of offline signature verification and also the challenges which are still present in this area.

Keywords: Biometrics; Handwritten Signatures; Deep Learning; Machine Learning; Offline; CNN

1. Introduction
In a large range of confidential applications, biometrics technology is used. The purpose of this type of systems is to identify an individual on the basis of behavioral and physiological characteristics. In case of physiological category, identifications are based upon the biological features measurement such as ears, fingerprints, iris, palm, and DNA, etc. Cognitive factors, such as expression, voice, gait, handwriting, and signature, are affected in the latter case. Also, handwritten signatures in the developing world remain a widely used and accepted method of biometric authentication [1].

1.1. Signature Verification
Any handwritten specimen of an individual's writing that specifies the first name, surname, nickname, or combination of the names used for identification purposes will be a signature [2]. The aim of the verification of the signature is to recognise the forged signature for reducing the risk of hacking and crime [3]. Procedure for signature’s verification has two main categories: Online Signature Verification and Offline Signature Verification, depending on the data acquisition technique. These two methods are also called, dynamic and static approaches respectively. In starting years signatures
were verified with the use of hand crafted features. But with the advent of deep learning in recent years there was a emergent attention in techniques that do not depend on hand-crafted feature extractors. As an alternative, raw data (pixels) is used in the case of images to learn feature representations [11]. The Deep Neural Network (DNN) is usually applied for solving the authentication, recognition or identification problems. Data such as writing speed and pen pressure using a digital device such as a tablet or stylus are included in the online process. This is dynamic data that can be documented in real-time. Whereas the Offline approach takes photographs of signatures collected by an optical scanner with a pen on paper [4].

![Figure 1: Types of Signature Verification (a) Online signature and (b) Offline signature](image)

1.2. Need of Signature verification

If the biometric sample is actually from a claimed person, the aim of the signature verification systems is to differentiate automatically. In simple words, this method is used to check whether the query signature is Genuine or Forge. Forgeries are categorized as Random Forgery, Unskilled Forgery/Simple, and Skilled Forgery in three key forms. In random forgeries, the forger is unaware of person’s name he has no knowledge of the person and his signature, and just uses his own signature. So for this type of situation, the forgery varies entirely from the actual one with a distinct overall form and design. In the case of Unskilled, sometimes referred to as basic forgeries, the forger knows the user's name, but not the user's signature. In this case, with a genuine signature, the forgery has a rather similar form and appearance. In instance of Skilled forgeries, the forger has complete information of name and signature of consumer and is well-practiced in imitating the signature. It is very difficult to detect this forgery as it looks exactly similar to the genuine signature [5].

There are several other forgeries in addition to these three types of forgeries: tracing, cut and paste, aimed, freehand and electronic forgery. There is less use for these forms of forgery. These are generally not considered in the literature.

1.3. Stages of Signature Verification

Data collection (also known as acquisition), pre-processing of data, extraction of features from data, and classification are typical signature verification measures. These are the key phases of the verification of signatures shown in Fig3.
1.3.1. Data Acquisition
Data acquisition applies to signature image capture [6]. For any verification process, this is the first and very significant step. Signature photographs are collected using a camera or optical scanner in the case of offline signature authentication.

1.3.2. Pre-Processing
Pre-processing is done to improve the quality of the image so that it can be efficiently applied to the feature extraction phase. Images may have blurry pixels, complex backgrounds, blurriness, and poor contrast for offline signature verification systems. Therefore, various pre-processing techniques have been applied to create an optimized image that can appropriate for other advanced tasks. The standard pre-processing steps include of signature extraction from whole image, background elimination, signature alignment, converting the signature into grayscale, removing noise or distortion with the help of some specific filters, normalizing the signature size, binarizing, normalizing the distance, skeletonizing, cropping and thinning, etc.

1.3.3. Feature Extraction
The features for signature verification can be static or dynamic. Static feature extracts the static information from signature images. Static information can be height, width, slant, density and baseline etc. These are taken into account in the case of offline signature authentication. In the case of authentication of online signatures, dynamic features are pen pressure, motion and speed as they are extracted at the time of signing. Statistical features can be further classified as Global features and Local features [7]. Global characteristics apply to a whole image of a signature or a representative of the whole image. Signature height, pure width, pure height, height to width ratio, picture, and maximum horizontal and vertical projection and so on are some of the global features. In local features, the signature image is separated in several equal parts (usually in 16 units) and from each specific segment features are extracted. Some local features are pixel density, distribution of pixels and axial slant. Local features can also be subdivides as pixel-oriented and component-oriented features.
1.3.4. Classification
Classification is the method for determining validity of the questioned signature. The most commonly used classification techniques are Support Vector Machine, Template Matching, Hidden Markov Model and Neural Networks or Deep Learning, etc.

1.4. Models for Signature verification
There are primarily two methods for developing offline signature authentication structures. Designing Writer-Dependent classifiers is the most widely used technique for signature verification. In this case, for each user, a training set is generated having positive examples which are genuine signatures and negative examples which are genuine signatures from other enrolled individuals. These way data is created and then on this dataset a classifier (binary) is trained, resulting in one model for each and every entity. This method has proven to perform quite well for the assignment, but as specially one individual model is needed for every enrolled user to be educated, so if there are increasing number of persons such as in bank this approach is not appropriate. Using a Writer-Independent approach is an alternate. In this case, for all users, a single model is trained in a space of dissimilarity by training a classifier. Classification inputs are vectors of dissimilarity, which represent the disparity between the query/questioned signature’s features and the prototype (A real user) signature’s features [8]. Engineering-based and Deep Learning-based approach is another categorization of the task to offline signature verification. Handcrafted characteristics are used in the engineering-based approach and automatically extracted from signature images in the deep learning-based approach [9].

![Figure3: Engineering based approach vs. Deep learning](image)

1.4.1 Engineering-based approach
It is based on hand-crafted features. In this case, features were extracted from the pre-processed image and applied to a specific classifier. Geometric characteristics, graphometric characteristics, directional characteristics, mathematical shifts, shadow-code, texture characteristics, interest point matching, pseudo-dynamic features are hand-crafted characteristics[28, 30, 31].

1.4.2 Deep Learning-based approach
In Deep Learning representation of features is learned from the raw data or pixels of images [1]. In deep learning, a neural network is trained to achieve the task of classification straight from text,
images and sound. These models can attain accuracy, even more than at the humans. These Models are educated with a huge array of labelled data also neural network architectures which include multiple layers.

The term "deep" commonly denotes to the amount of layers which are hidden in the neural network. In old-style neural networks, there are only 2-3 hidden layers, while deep neural networks can include as many as 250 layers.

With the use of very wide sets of labelled data and also the neural network architectures in which features are learned from the data, deep learning models are trained without the need for manual extraction of features.

A subpart of DNN that includes multiple layers is the Convolution Neural Network (CNN), where each layer performs some pre-assigned and unique role. The network can acquire features only from input image, and a feature vector for categorizing between pairs of signatures can also be acquired [10].

1.5 Performance Parameters

(A) False Acceptance Rate (FAR): It is defined as proportion of the amount of forge signature recognized as a genuine signature to the total amount of forge signature submitted as shown in the equation (1)

\[ FAR = \frac{FP}{FP + TN} \]  (1)

Where FP: False positive (observation is negative but predicted as positive)
FN: False Negative (observation is positive but predicted as negative)
TN: True Negative (observation is negative but predicted as negative)
TP: True Positive (observation is positive but predicted as positive)

(B) False Rejection Rate (FRR): It is defined as the percentage of the number of genuine signatures accepted as a forged signature to the total number of genuine signature submitted as shown in equation (2)

\[ FRR = \frac{FN}{FN + TP} \]  (2)

(C) Accuracy (ACC): Accuracy is a measure of correct predictions. It a ratio of all true positive and true negative to all possible cases as shown in equation (3)

\[ ACC = \frac{TP + TN}{TP + FP + TN + FN} \]  (3)

(D) Equal Error Rate (EER): As number of false acceptances (FAR) decreases, the number of false rejections (FRR) will increase and vice versa. The point where this two intersects is called Equal Error. At this points the percentage of FAR and FRR are equal.
Figure 4: Equal Error Rate

(E) Average Error Rate (AER): This is defined as the average of FRR and FAR as can be seen in equation (4)

\[
AER = \frac{FAR + FRR}{2}
\]

1.6 Publically Available Datasets for Offline Signature Verification

For offline and online signature authentication, there is a wide range of publicly accessible datasets. Some datasets for offline signature verification are listed in table 1. The table includes the dataset name, number of users and also the number of real and forged signatures per user, and the output parameters for each dataset.

| Reference Number | Data-set Name          | No. of users | No. of Genuine signatures per user | No. of Forged signatures per user | Total no. of signature images in data-set | Performance |
|------------------|------------------------|--------------|-----------------------------------|-----------------------------------|------------------------------------------|-------------|
| [1]              | MCYT                   | 75           | 15                                | 15                                | 2250                                     | ACC: 90.78% |
| [1]              | CEDAR                  | 55           | 24                                | 24                                | 1344                                     | EER: 100%   |
| [1]              | UT Sig                 | 115          | 27                                | 45                                | 8280                                     | EER: 6.17%  |
| [1]              | Brazilian (PUC-PR)     | 60 and 108   | 40                                | simple forgery-10                 | 10080                                    | EER: 1.48%  |
The paper is organized as section 2 describes the literature survey, section 3 defines the challenges in the offline signature verification for these challenges proposed methodology is described in section 4, section 5 contains expected outcomes and finally section 6 conclude the whole paper.

2. Literature Survey
Signature Verification is an old concept. It has been researched for more than 30 years. In starting, signatures were manually checked, which is not an accurate method for this task. In the 20th century, computers were invented, experts tried to build new methods for verifying signatures more accurately as compared to traditional methods. Since 1960, information technology has been working in signature verification.[22]. North America Aviation proposed the first electronic signature verification method in 1965[23]. The research in the field of online signature recognition was first published by Mauceri in the same year.[23]. Kozinets et al.[24] first used computers in the 1966 off-line verification method for the first time. In 1973, the first algorithm for offline signature verification were published in the IEEE Conference and Transaction by Nagel and Rosenfeld[25]. A Pseudo-dynamic feature extraction technique was proposed by Ammar et al. in 1986 to extract pressure information from grayscale images.[26]

| Ref | Journal/conference | Dataset | Features | Technique | Performance |
|-----|---------------------|---------|----------|-----------|-------------|
| [16] | GPDS 160            | 160     | 24       | 30        | 8640        | EER: 0.69%  |
| [17] | GPDS 960            | 960     | 24       | 30        | 47574       | EER: 22.76% |
| [18] | SigComp2011(Dutch)  | 64      | 24       | 12        | 2295        | ACC: 94.37% |
|     | SigComp2011(Chinese)| 20      | 24       | 34        | 1176        | ACC: 99.96% |
| [19] | SigWiComp2013(Dutch)| 27      | 10       | 36        | 1241        | ACC: 81.76% |
|     | SigWiComp2013(Japanese)| 20   | 42       | 36        | 1566        | ACC: 93.39% |
| [20] | BHSig 260(Hindi)    | 160     | 24       | 30        | 8640        | ACC: 95.40% |
|     | BHSig 260(Bangla)   | 100     | 24       | 30        | 5400        | ACC: 97.77% |
| [21] | GPDS Synthetic      | 4000    | 24       | 30        | 120024      | ACC: 86.47% |
| Reference | Year | Journal/Conference/Workshop | Number | Parameters                                                                 | Method | Accuracy/EER |
|-----------|------|-----------------------------|--------|-----------------------------------------------------------------------------|--------|---------------|
| [27]/2011 |      | Procedia computer science   | 100    | Area, Centre of gravity, Eccentricity, Kurtosis and Skewness               | ANN    | ACC: 93%      |
| [28]/2011 |      | 2011 International Joint Conference on Biometrics (IJCB) | GPDS 160 | local binary patterns(LBP) and histogram of oriented gradients(HOG)        | Global SVM and User dependent SVM | EER:15.41% |
| [29]/2012 |      | International Journal of Engineering and Research Technology(IJER) | Persian signature signature images | Textures features(LBP)                                                     | CNN    | ACC: 99.86%   |
| [30]/2012 |      | IEEE Transactions on Information Forensics and Security (Volume: 7, Issue: 3, June 2012) | MCYT, GPDS960 | SVM                                                                         | EER:24.78% |
| [31]/2013 |      | International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013 | personal dataset created Pixels | Pixel matching technique (PMT)                                             | ACC: 94% |
| [32]/2014 |      | International Journal of Machine Learning and Computing, | 646 reference and 1287 question signatures | time series shapelets                                                       | Mahalanobis distance | EER: 5.8% |
| Year | Conference/Source | Type | Features | Classifiers | Results |
|------|------------------|------|----------|-------------|---------|
| 2014 | Springer         | GPDS-160 | gravity center point, feature graph | ACC: 17.4% |
| 2014 | 2014 Fifth International Conference on Signal and Image Processing | 336 signature | Gravity center, loops count measured, horizontal/vertical profiles and calculated normalized area, centroid | SVM | EER: 7.16% |
| 2015 | Pattern Recognition | GPDS-160 and CEDAR | Curvelet transform (Genuine signature only) | one class SVM (OCSVM) | AER: 16.92% |
| 2015 | International Journal Of Innovations In Engineering, Research And Technology | 1000 signature images | signature images | Neural Networks | ACC: 86.25% |
| 2016 | IEEE Transactions on Information Forensics and Security | CEDAR, GPDS 300 | Directional Code Co-occurrence matrix (DCCM) | One-class writer-independent method utilizing tests of feature dissimilarity (FDM) classification thresholds and a smaller number of references | AER: 18.42% |
| Year | Conference | Dataset | Features | Model | Accuracy/Metric |
|------|------------|---------|----------|-------|----------------|
| 2016 | Pattern Recognition Letters | UTSig, MCYT-75 and GPDS960 GraySignatures | Discrete Radon Transform (DRT) features and Histogram of Oriented Gradients (HOG) | deep multitask metric learning (DMML) | EER:20.94%, 15.08%, 22.76% |
| 2016 | Advances in Visual Computing | Dutch, ICDAR SigWiComp 2013 dataset | triplets of two genuine and one forged signature | CNN(10 conv. layer) and Euclidian distance | ACC:dutch-81.76, ICDAR-93.39% |
| 2016 | Pattern Recognition Letters | ICDAR 2011 SigComp dataset | Signature images | VGG16 | Accuracy: 97%dutch, 95%chinese |
| 2017 | Pattern Recognition Letters | GPDS-160, MCYT, CEDAR and Brazilian PUC-PR datasets | Signature images | CNN (5 conv. Layer) and SVM classifier | EER:1.72, 2.87, 4.63, 2.01 |
| 2017 | Pattern Recognition Letters | CEDAR, GPDS300, GPDS synthetic, Bengali, Hindi | Signature images | Siamese Neural Network (Euclidian distance) | ACC: CEDAR-100%, GPDS300-76.83%, GPDSsynthetic-77.76%, Bengali-86.11%, Hindi-84.64% |
| 2018 | Pattern Recognition Letters | MCYT, GPDS synthetic and CEDAR | local features (angle, centroid, distance and slope) and Global features (area, aspect ratio, pure height, pure width and | Best feature selected with the help of Genetic algorithm and used ANN and SVM for classification | AER: 7.88, 12.50 and 5.95 |
| Year | Proceedings | Authors | Signature Images | Methods | ACCs |
|------|-------------|---------|------------------|---------|------|
| 2018 | International Conference on Recent Trends in Image Processing and Pattern Recognition | GPDS synthetic, MCYT-75 | Signature images | Siamese Neural Network | ACC: 84.58%, GPDS, 85.38% MCYT |
| 2018 | International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism | GPDS synthetic | Signature images | CNN | ACC: 62.5%, WD-75% |
| 2019 | International Journal of Technology and Human Interaction | GPDS synthetic(185 user- 4070), BME2(31 user-860), SVC20(20user-360) | Signature images | CNN and for classification cubic SVM | ACC: 97.7%, 99.4%, 100% |
| 2019 | Procedia Computer Science | GPDS(1000 users) | Signature images | Inception v1 & v3 | ACC: inception V1-83%, inception V3-75% |
| 2019 | 2019 Fifth International Conference on Image Information Processing (ICIIP) | CEDAR, BHSig260 signature corpus, and UTsig. | Signature images | CNN(inception v-1) | ACC: CEDAR-100%, BH260 hindi-95.40, benagali-97.77%, UT sig-80.44% |
| 2020 | Applied Sciences | ICDAR 2011 SigComp | Signature images | Explainable Deep learning | ACC:94.37% to 99.96% |
| 2020 | Multimedia | GPDS- | Signature | Siamese | ACC: 86.47 |
3. Challenges
From the literature it has been observed that offline signature verification has three major challenges:

- The biggest challenge in the process of signature verification is signatures have very high intra-class variations. Since a person’s signature depends on some factors like mood, age, mental stress, physical conditions, and time so there can be many variations in signatures produced by the same person. It makes the task of signature verification more complex [1, 2, and 44].

- The existence of partial information during training is another major challenge in the training of signature verification system [1, 10].

- The amount of information is very limited in real-life applications [45]

These issues can be overcome by using GPDS synthetic dataset which has 4000 synthetic users and each user consist of 30 forge signatures and 24 genuine. This dataset is created by combining GPDS960 and MCYT dataset. Synthetic signatures are created using some specific algorithms [21]. It is largest dataset for offline signature variation which is publically aviable. Henceforth, mitigates the above-mentioned limitations. Many kinds of research have been done so far on this dataset but still, scope is open for the researchers [10, 46].

4. Proposed Methodology
First of all, the dataset will be acquired, this is data acquisition. After that some preprocessing steps such as data resizing, data normalization will be performed. Then data set will be split into training and testing data. After that, a CNN model will be applied and their performance will be evaluated. As shown in figure 5.
5. Results & Discussion
The results can be expressed in terms of EER (Equal Error Rate), AER (Average Error Rate) and Accuracy. By applying the proposed CNN-based model for offline signature verification improved accuracy and a reduced error rate can be achieved. As it can be seen from the literature that CNN models can increase the accuracy of the system, so if a more advanced model will be used for Offline Signature Verification results can be improved. Results can also be improved by using a large scale database GPDS synthetic which has 120024 signature images from 4000 users having 24 genuine and 30 forge signatures per users. It is the largest publically available dataset for offline signature verification. It can handle the challenges in the task of offline signature verification such as high intraclass variability, having knowledge of only genuine signature of the user and also having small number of sample in real life applications. So, In future we will make use of GPDS synthetic dataset and apply it to a more advanced CNN model whether it can be Siamese neural network, transfer learning model, or any combination of these techniques.

6. Conclusion and Future Work
Offline signature verification is used in many applications areas so there is a need for a system which can correctly identify genuine signature from forged signatures. In this paper we have discussed various needs of signature verifications, its types and various approaches or models which can be
applied for this task. We have also described the work done by the researchers in last 3 decades. Many techniques have been applied for this task whether engineering based or deep learning based. Recently, there has been growing interest in methods that are based on Deep Learning because they learned from the raw data or pixels. So for future work, deep learning based methods such as Convolutional Neural Network, Siamese Network (also called as one shot learning) and transfer learning techniques can be applied for the purpose of offline signature verification.

REFERENCE

[1] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017, November). Offline handwritten signature verification—Literature review. In 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-8). IEEE.

[2] Bibi, K., Naz, S., & Rehman, A. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79(1), 289-340.

[3] Maergner, P., Pondenkandath, V., Alberti, M., Liwicki, M., Riesen, K., Ingold, R., & Fischer, A. (2019). Combining graph edit distance and triplet networks for offline signature verification. Pattern Recognition Letters, 125, 527-533.

[4] Sharif, M., Khan, M. A., Faisal, M., Yasmin, M., & Fernandes, S. L. (2018). A framework for offline signature verification system: Best features selection approach. Pattern Recognition Letters.

[5] Soleimani, A., Araabi, B. N., & Fouladi, K. (2016). Deep multitask metric learning for offline signature verification. Pattern Recognition Letters, 80, 84-90.

[6] Dimauro, G., Impedovo, S., Lucchese, M. G., Modugno, R., & Pirlo, G. (2004, October). Recent advancements in automatic signature verification. In Ninth International Workshop on Frontiers in Handwriting Recognition IEEE. (pp. 179-184).

[7] Impedovo, D., Pirlo, G., & Russo, M. (2014, September). Recent advances in offline signature identification. In 2014 14th International Conference on Frontiers in Handwriting Recognition IEEE. (pp. 639-642).

[8] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70, 163-176.

[9] Al-Omari, Y. M., Abdullah, S. N. H. S., & Omar, K. (2011, June). State-of-the-art in offline signature verification system. In 2011 International Conference on Pattern Analysis and Intelligence Robotics IEEE. (Vol. 1, pp. 59-64).

[10] Jagtap, A. B., Sawat, D. D., Hegadi, R. S., & Hegadi, R. S. (2020). Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). MULTIMEDIA TOOLS AND APPLICATIONS.
[11] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *nature, 521*(7553), 436-444.

[12] Julian Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and Javier Ortega-Garcia (2004). An off-line signature verification system based on fusion of local and global information. In *Biometric Authentication, Springer* pages 295-306.

[13] Meenakshi K. Kalera, Sargur Srihari, and Aihua Xu. (November 2004) Offline signature verification and identification using distance statistics. *Int. Journal of Pattern Recogn., 18*(07):1339–1360.

[14] SoleimaniA, FouladiK, AraabiBN (2016) Utsig: A persian offline signature dataset. *IETBiom* 6(1):1–8

[15] C. Freitas, M. Morita, L. Oliveira, E. Justino, A. Yacoubi, E. Lethelier, F. Bortolozzi, and R. Sabourin.(2000) Bases de dados de cheques bancarios brasileiros. In *XXVI Conferencia Latinoamericana de Informatica,*

[16] M. A. Ferrer, J. B. Alonso, and C. M. Travieso.(June 2005) Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 27*(6):993–997.

[17] J.F. Vargas, M.A. Ferrer, C.M. Travieso, and J.B. Alonso. (September 2007) Off-line Handwritten Signature GPDS-960 Corpus. In *Ninth International Conference on Document Analysis and Recognition, ICDAR 2007,* volume 2, pages 764–768, 2007.

[18] Liwicki M, Malik MI, van den Heuvel CE, Chen X, Berger C, Stoel R, Blumenstein M, Found B (2011) Signature verification competition for online and offline skilled forgeries (sigcomp2011). In: *2011 international conference on document analysis and recognition (ICDAR), IEEE* pp 1480–1484.

[19] Malik, M.I., Liwicki, M., Alewijnse, L., Ohyama, W., Blumenstein, M., Found, B(2013): ICDAR 2013 competitions on signature verification and writer identification for on-and offline skilled forgeries (SigWiComp 2013). In: *2013 12th International Conference on Document Analysis and Recognition, IEEE* pp. 1477–1483.

[20] S. Pal, A. Alaei, U. Pal, M. Blumenstein,(2016,) Performance of an off-line signature verification method based on texture features on a large indic-script signature dataset, in: *DAS, pp. 72–77.

[21] M.A. Ferrer, M. Diaz-Cabrera, and A. Morales (June 2013) Synthetic off-line signature image generation. In *2013 International Conference on Biometrics (ICB), pages 1–7.*

[22] Fauziyah, S., Azlina, O., Mardiana, B., Zahariah, A. M., & Haroon, H. (2009, March). Signature verification system using support vector machine. In *2009 6th International Symposium on Mechatronics and its Applications, IEEE.* (pp. 1-4).

[23] Gupta, N., & Saravanan, K. (2017). Comparative study of various signature verification algorithms. *International Research Journal of Engineering and Technology, 4*(4).
[24] Thakare, B., Deshmukh, H., & Mahalle, P. (2016). Handwritten signatures: An understanding. *International Journal of Computer Applications*, **139**(4), 21-26.

[25] Nagel, R. N., & Rosenfeld, A. (1973, October). Steps toward handwritten signature verification. In *Proc. First Int. Joint Conf. on Pattern Recognition, Washington, DC* (pp. 59-66).

[26] Yeung, D. Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., & Rigoll, G. (2004, July). SVC2004: First international signature verification competition. In *International conference on biometric authentication, Springer, Berlin, Heidelberg* (pp. 16-22).

[27] Karouni, A., Daya, B., & Bahlak, S. (2011). Offline signature recognition using neural networks approach. *Procedia Computer Science*, **3**, 155-161.

[28] Yilmaz, M. B., Yanikoglu, B., Tirkaz, C., & Kholmatov, A. (2011, October). Offline signature verification using classifier combination of HOG and LBP features. In *2011 international joint conference on Biometrics (IJCB)* IEEE. (pp. 1-7).

[29] Khalajzadeh, H., Mansouri, M., & Teshnehlab, M. (2012). Persian signature verification using convolutional neural networks. *International Journal of Engineering Research and Technology*, **1**(2), 7-12.

[30] Ferrer, M. A., Vargas, J. F., Morales, A., & Ordonez, A. (2012). Robustness of offline signature verification based on gray level features. *IEEE Transactions on Information Forensics and Security*, **7**(3), 966-977.

[31] Bhattacharya, I., Ghosh, P., & Biswas, S. (2013). Offline signature verification using pixel matching technique. *Procedia Technology*, **10**, 970-977.

[32] Arathi, M., & Govardhan, A. (2014). An efficient offline signature verification system. *International Journal of Machine Learning and Computing*, **4**(6), 533.

[33] Neamah, K., Mohamad, D., Saba, T., & Rehman, A. (2014). Discriminative features mining for offline handwritten signature verification. *3D Research*, **5**(1), 1-6.

[34] Kruthi, C., & Shet, D. C. (2014, January). Offline signature verification using support vector machine. In *2014 Fifth International Conference on Signal and Image Processing* IEEE. (pp. 3-8).

[35] Guerbai, Y., Chibani, Y., & Hadjadji, B. (2015). The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. *Pattern Recognition*, **48**(1), 103-113.

[36] Hatkar, P. V., Salokhe, B. T., & Malgave, A. A. (2015). Offline handwritten signature verification using neural network. *Methodology*, **2**(1), 1-5.

[37] Hamadene, A., & Chibani, Y. (2016). One-class writer-independent offline signature verification using feature dissimilarity thresholding. *IEEE Transactions on Information Forensics and Security*, **11**(6), 1226-1238.
[38] Rantzsch, H., Yang, H., & Meinel, C. (2016, December). Signature embedding: Writer independent offline signature verification with deep metric learning. In *International symposium on visual computing Springer, Cham.* (pp. 616-625).

[39] Soleimani, A., Araabi, B. N., & Fouladi, K. (2016). Deep multitask metric learning for offline signature verification. *Pattern Recognition Letters, 80, 84-90.*

[40] Alvarez, G., Sheffer, B., & Bryant, M. (2016). Offline signature verification with convolutional neural networks. *Technical report, Stanford University.*

[41] Dey, S., Dutta, A., Toledo, J. I., Ghosh, S. K., Lladós, J., & Pal, U. (2017). Signet: Convolutional siamese network for writer independent offline signature verification. *arXiv preprint arXiv:1707.02131.*

[42] Jagtap, A. B., Sawat, D. D., Hegadi, R. S., & Hegadi, R. S. (2018, December). Siamese Network for Learning Genuine and Forged Offline Signature Verification. In *International Conference on Recent Trends in Image Processing and Pattern Recognition Springer, Singapore.* (pp. 131-139).

[43] Yapici, M. M., Tekerek, A., & Topaloglu, N. (2018, December). Convolutional neural network based offline signature verification application. In *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELT) IEEE.* (pp. 30-34).

[44] Jagtap, A. B., Hegadi, R. S., & Santosh, K. C. (2019). Feature learning for offline handwritten signature verification using convolutional neural network. *International Journal of Technology and Human Interaction (IJTHI), 15(4), 54-62.*

[45] Sam, S. M., Kamardin, K., Sjarif, N. N. A., & Mohamed, N. (2019). Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3. *Procedia Computer Science, 161, 475-483.*

[46] Mohapatra, R. K., Shaswat, K., & Kedia, S. (2019, November). Offline handwritten signature verification using cnn inspired by inception v1 architecture. In *2019 Fifth International Conference on Image Information Processing (ICIIP) IEEE.* (pp. 263-267).

[47] Kao, H. H., & Wen, C. Y. (2020). An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach. *Applied Sciences, 10(11), 3716.*