International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 6, September-October 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Comprehensive Review of Offline Signature Verification Mechanisms

Shilpee Agrawal[1], Dr. Mohd Ahmed[2]

[1]Research Scholar, [2]Professor,
[1,2]Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

One of the oldest and most well-known biometric testifying procedures in modern culture is the authentication of handwritten signatures. The field is divided into areas that operate online and offline depending on the acquisition procedure. In online signature verification, the entire signing procedure is carried out using some sort of acquisition equipment, whereas offline signature verification just uses scanned photographs of the signatures. In this paper, we propose an image-based offline signature realization and verification system. Support Vector Machine and artificial neural network are both employed to support the goal intended for this thesis. Modern better processes for features extraction are presented. Two independent sequential neural networks are created, one for verifying and the other for recognizing signatures (i.e. for detecting forgery). A recognition network regulates the parameters of the verification network, which are generated separately for each signature. A signature code and acceptable dataset are used to rigorously validate the System's overall performance.

KEYWORDS: *Offline signature verification, GPDS, Hus Moment, Radon Transform, ANN, SVM*

How to cite this paper: Shilpee Agrawal | Dr. Mohd Ahmed "Comprehensive Review of Offline Signature Verification Mechanisms" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-6, October 2022, pp.876-881, URL: www.ijtsrd.com/papers/ijtsrd51950.pdf

IJTSRD51950

1. INTRODUCTION

Rapid increases in processing power have occurred as a result of technical advancements. This has made it possible for computers to run intricate and comprehensively computational programmes more quickly. This progression has led to an increase in demand for automated systems, which might reduce the need for labour. Thus, it is possible to create precise and quick matching systems to take advantage of these technological improvements. Signature matching biometrics are less often studied than other types of biometrics. Since humans have been using their signatures as a kind of identification verification for thousands of years, this is common. A important approach for preventing fraud in financial transfers and security concerns is biometric authentication. Particularly, the verification of handwritten signatures in financial transactions has been employed extensively. Due to this requirement, the study of signature matching has become quite popular. The phrase "signature" refers to the act of writing one's name, initials, or even a particular letter, such as a "A," on a piece of paper. In relation to signatures, the word "autograph" is sometimes used interchangeably with "signature," however it really refers to an artistic signature. When people have both of them, which include their signature and autograph, still another complication arises. Such individuals totally reveal their autograph while keeping their autographs concealed. When compared to qualities that fall within the category of physical attributes like iris, face, finger print, etc., a signature exhibits a larger intra class and temporal variability, making it an observable biometric that hides the signer's ballistic movement, which is challenging to mimic. While signatures are a biometric of interest because to their wide range of uses in both the public and specialist markets, such as applications for banking, verifying papers, and document confirmation. Figure 1.1 depicts a trademark usage pattern.

Fig 1. Signature Example

Signatures can be interpreted in many different ways and used for a variety of things, including proving someone's physical existence (such as when they sign in for work), gathering witnesses (such as when they sign a contract), sanctioning or authorising something with a seal, and validating something with a stamp. Each person or item has their own individual writing and signing style that is frequently fairly recognisable.

1.1. Different Types of Systems

A distinguishing quality for identifying people has been their signature. Even now, a growing number of transactions, particularly those involving money and commerce, are being approved by signatures. Therefore, it is vital to create techniques for automatic signature verification if dependability is to be properly checked and ensured on a regular basis. In particular, offline and online signature verification are the two methods used for signature authenticity. Online signature is a biometric used to manage access to facilities, get access to locations that are guarded for surveillance purposes, and for personal identification for security. Offline signature authentication is more difficult than online signature verification because of differences between user signatures and the ease with which the position of the signature may be examined. Both offline and online signature verification provide a great deal of difficulty. For example, instructions like the availability of non-static information restrict the number of signatures that may be copied and make the process considerably more difficult. Aside from some signatures that are really clear, securing both the non-static information and shape of a signature that is online suggests to be a little hard

2. Literature Review

2.1. Early works

The problem of offline signature verification has been thoroughly investigated, and several interesting approaches have been examined. There are initial evaluations available that address early advancements in the subject. In a paper by Coetzer [1], an analysis of suggested works is presented. The initial step is to extract the signature area of interest from a document before using further applications like verification or recognition. This step is often bypassed in studies that focus on biometric applications of signatures. However, a small number of research that focus on signature localisation may be found in the literature. Analysis of the connection between handwriting and signature [2] Bouletreau et al. Both handwriting and signature categorization that depends on their fractal behaviour may use a Process. Chalechale et al. [3]'s work focuses mostly on extracting signature regions from documents. 350 papers in a database of document images, each of which was signed by 70 distinct Cursive signatures in Persian or Arabic are used by people. The photos include a range of mixed text in various fonts and sizes in Arabic, Persian, and English, as well as a corporate logo, some horizontal and vertical lines, and a cursive signature. In 346 instances (98.86%), the signature area was successfully located, and in 342 cases, the whole signature was recovered (97.71 percent). This is because the algorithm focuses on nearby link segments, yet certain cursive signatures include significant disconnected areas.

According on the number of embellishments in a signature, Alonso et al. classified signatures [4]. According to the kind of their signatures, users are divided into four categories: simple flourish (C1), complicated flourish (C2), simple flourish with name (C3), and complex flourish with name (C4) (C4). Figure 1 displays sample signatures from each group. 3. According to the MCYT-75 corpus [5], the distribution of users is as follows: C1 (6.67%), C2 (17.33%), C3 (46.67%), and C4 (29.33 percent). EERs are ranked from lowest to highest as C4, C2, C3, and C1 using the HMM verifier of local information. The addition of the user name information makes the signature considerably more difficult to copy, which is the predicted outcome given that complicated drawings make signatures more difficult to copy. Two signatures (a query and a reference) are first aligned using rigid or non-rigid alignment in a study by Nguyen et al.[7] and then they are compared using general characteristics that may be retrieved from the whole signature, such as the width/height ratio or pixel density .It is intended that this alignment will account for differences in rotation, translation, and scale. Pal et al. [6] provide a multi-script signature identification method. The Bengali (Bangla), Hindi (Devanagari), and English signatures are taken into consideration for the identification procedure in the proposed signature identification system. In their analysis of the resistance of offline signature verification to various

influencing circumstances, Ferrer et al[8]. The innovative component is imitating actual bank checks by varying the amount of noise that is added to signature photos. The baseline verification approach is derived from Porwik et al.[9] (2016) suggested a biometric technique based on the properties of a signature. Features of a signature are individually matched to a given signature using suitable similarity coefficients, and compounded features may be decreased as needed. In [10], authors employed offline handwritten signature verification using low level stroke features that were first presented for the identification of printed Gujarati text. The ICDAR 2009 Signature Verification Competition dataset, which includes both real and fake signatures, was used for the experiment. Support Vector Machine (SVM) classifier with three-fold cross validation is used for recognition. The Equal Error Rate (EER) of 15.59 obtained is similar to the results of the ICDAR 2009 Signature Verification Dataset. [11] examines how well the Local Binary Pattern feature set and the k-Nearest Neighbors classifier work together to provide an offline signature verification system that is writer independent. Two signature databases with 100 and 260 authors each are utilised to assess the system's performance.[12] evaluated using an Artificial Neural Network and a Local Binary Pattern feature set. Utilizing two datasets of signatures, each containing 260 and 100 authors, the system's performance is assessed.

In [13], the authors present a one-class WI system with a decreased number of references and feature dissimilarity measures thresholding for classification. The suggested system makes use of a directional code co-occurrence matrix feature generating technique based on contourlet transforms.

In [14], an ensemble-based technique is provided, which combines a method for creating an ensemble of features utilising geometrical and Mobile Net characteristics with an ensemble of classifiers. The technique has been examined using the readily accessible dataset BHSig260.

3. Implementation and Methodology

The goal of this paper is to develop an offline mechanism for signature verification and qualitatively discuss and evaluate the findings in relation to the numerous methods that are accessible at each stage of the process. With the aim of conducting a comparative study of the various offline signature verification techniques now in use, the algorithms and processes chosen have been evaluated on three distinct databases.

Numerous databases are accessible and are used to validate signatures. A list of some of the most popular major databases is provided below.

TABLE 1.1 USED DATASETS

Data set name	Users	Genuine Signatures	Forgeries
CEDAR [36]	55	24	24
MCYT-75 [20]	75	15	15
GPDS Signature 160 [17]	160	24	30
GPDS Signature 960 Grayscale [62]	881	24	30
GPDS Synthetic Signature[19]	4000	24	30
Brazilian (PUC-PR) [21]	315	40	10 simple, 10 skilled

3.1. Data Processing Steps

1) Data gathering and preparation 2) The processes below are carried out for feature extraction.

First Hu's is applied on the original signature to receive 7 features as a result. The signature picture is then given a 1D radon transformation. 35 features will be calculated by performing the 2D radon function in 4 directions (0, 45, 90, and 135).

The Hus moment is once again applied in this direction after receiving 1D radon pictures. The original signature is then divided vertically into 4 zones. This is accomplished by normalising the signature to a size of 32*128 such that one zone's size after zoning is 32*64. Then, the Gabor wavelet is applied to each zone in six different directions (0, 30, 60, 90, 120, and -30). Energy and Standard Deviation (STD) is calculated for each sub band independently (will get 48 features). As the last stage in feature extraction, Hu's moment is once again applied to each zone after obtaining Gabor wavelet pictures. The closest neighbour classifier is employed throughout the identification steps. In order to compare the performance of ANN and Support Vector Machine (SVM) as classifiers, we calculated results for verification.

4. Results

The first test set has 16 genuine signatures of this person and 8

Fig 2 Screenshot from test set of genuine signatures

The Hu's Transform and Radon Transforms are two feature extractors that are used by the system to scan over the whole dataset of training and test pictures and extract features. When an ANN is employed as a classifier, the system uses the ANN tool to train the network to perform according to the training set's signature test set and a defined objective. To identify the system's optimal performance scenario, we evaluated it against various performance objectives and epochs.

Results from the GPDS Signature Set

The GPDS Signature 160 consists of 160 users with 24 genuine users and 30 forged users. The test data set was further bifurcated into 3 subsets based on the classification of type of signature category the signature belongs to typically simple, cursive or Graphical. The Performance analysis and calculation of performance analysis parameters was done.

TABLE 1.2 TYPES OF SIGNATURE

Database	Simple	Cursive	Graphical
GPDS Signature synthetic offline and online data set	34	95	31

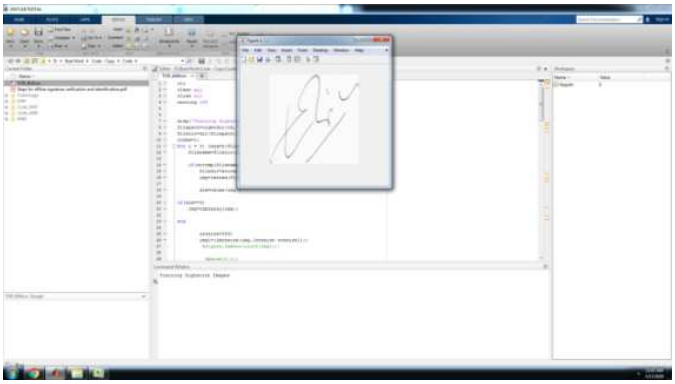


Fig 3: MATLAB testing platform using the GPDS dataset and an ANN as a classifier

Fig 4: Test signature image after Transform

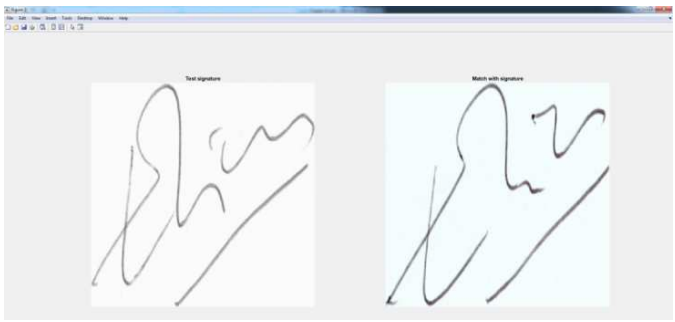
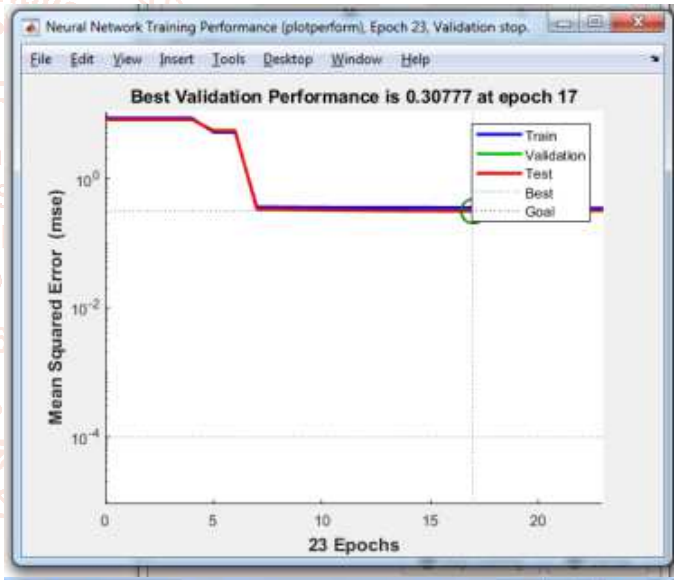


Fig 5: Extracted signature with the least distance as per nearest neighbor distance algorithm and ANN as verification classifier



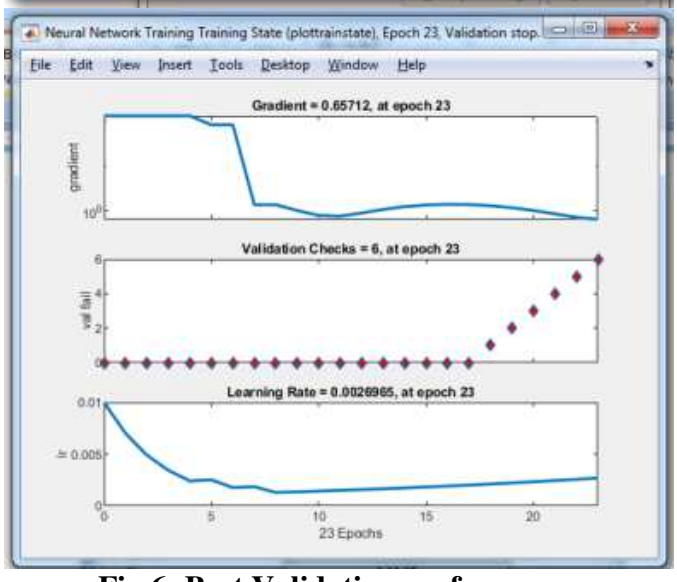


Fig 6: Best Validation performance

4.1. Performance analysis for Simple Signatures

Simple signatures are the ones where the person just writes his or her name. The GDPS database was analysed and we separated 34 signatures to be simple based on the ease 10 Sample forgerers were able to imitate these signatures to a degree of being classified as genuine forgery or at minimum skilled forgery. All of these 34 users have 12 samples (408 total signatures in the set) each out of which 6(204 in total set) are genuine and 6(204) forged. So each classified subset is further classified into sample and forged signature dataset. The performance evaluations are on the basis of these parameters

The system is trained using the ANN Classifier

The Training is done using the entire data set of Genuine and forged Signatures for a particular group of Simple Signatures.

If the test Sample signature is taken from the Genuine Data subset, and the system exactly picks up the same signature from the genuine dataset or matches it with any other signature from the genuine dataset only, it is considered as a HIT.

If the test Sample signature is taken from the Forged Data subset, and the system exactly picks up the same signature from the forged dataset or matches it with any other signature from the forged dataset only, it is also considered as a HIT.

If the test Sample signature is taken from the Genuine Data subset, and the system matches it with any other signature from the forged dataset, it is considered as a MISS. This number of genuine signatures taken as forged signatures and hence discarded by the system, will be used in the calculation of FRR.

If the test Sample signature is taken from the Forged Data subset, and the system matches it with any other signature from the genuine dataset, then also it is considered as a MISS. This number of forged signatures taken as genuine signatures and hence accepted by the system, will be used in the calculation of FAR.

TABLE 1.3 RESULTS OF COMPUTATION OF SIMPLE SIGNATURE DATABASE FOR GENUINE SIGNATURES

Type of Signature	Genuine Signatures matched with Exact/Genuine set	Genuine Signatures matched with Forged Dataset (False rejection)
Simple	196/204	8/204

False Rejection rate = Genuine signatures discarded/Total Genuine Signatures tested= $\frac{8}{204} * 100 = 3.921$

TABLE 1.4 RESULTS OF COMPUTATION OF SIMPLE SIGNATURE DATABASE FOR FORGED SIGNATURES

Type of Signature	Forged Signatures matched with Exact/Forged set	Forged Signatures matched with Genuine Dataset (False rejection)
Simple	189/204	15/204

False Acceptance rate = Forged signatures accepted/Total Forged Signatures tested= $\frac{15}{204} * 100 = 7.35$

TABLE 1.5 RESULTS OF COMPUTATION OF CURSIVE DATABASE USING ANN

Type of Signature	Genuine Signatures matched with Exact/Genuine set	Genuine Signatures matched with Forged Dataset (False rejection)
Cursive	95/108	13/108

False Rejection rate = Genuine signatures discarded/Total Genuine Signatures tested= $\frac{13}{108} * 100 = 12.03$

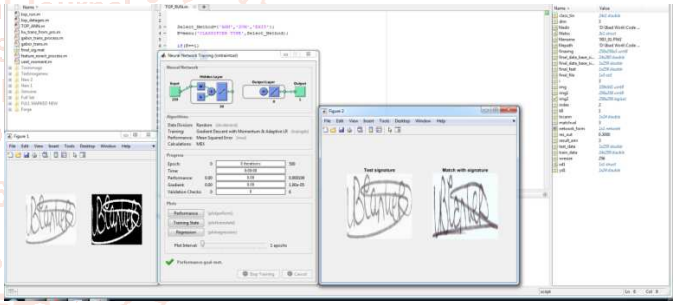


Fig 7 Example of Genuine signature matched with forged signature thereby resulting in rejection and contributing to false rejection rate

TABLE 1.6 ANALYSIS OF FORGED SIGNATURES

Type of Signature	Forged Signatures matched with Exact/Forged set	Forged Signatures matched with Genuine Dataset (False rejection)
Cursive	92/108	16/108

False Acceptance rate = Forged signatures accepted/Total forged Signatures tested= $\frac{16}{108} * 100 = 14.81$

5. Conclusions

The GDP Database was used for the decisive conclusions. However other databases have also been used with significant success using the proposed mechanisms. However the GDPS dataset provided the

option of classifying the systems on the basis of types of signatures available in the dataset on the basis of type of signature i.e Simple, Cursive and Graphical. The reason for this classification was testing and classifying the system performance based on the type and structural complexity of the signature. The performance of system has been evaluated on the basis of standard signature recognition parameters i.e False Error Rate and False Recognition rate. Parameters like EER were not utilized for any concrete decision making. The results have been compared with most of the recent works and have been found to fair reasonably well as compared to the existing mechanisms with the use of proposed mechanisms in this works.

References

[1] J. Coetzer, "Off-line signature verification," Ph. D. dissertation, University of Stellenbosch, South Africa, 2005

[2] V. Bouletreau, N. Vincent, R. Sabourin, and H. Emptoz, "Handwriting and signature: one or two personality identifiers?" in Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on, vol. 2, Aug 1998, pp. 1758–1760 vol. 2

[3] A. Chalechale, G. Naghdy, P. Premaratne, and A. Mertins, "Cursive signature extraction and verification," in Proc. 2nd Int. Workshop on Information Technology & Its Disciplines (WITID 2004), Kish Island, Iran, July 2004, pp. 109–113.

[4] F. Alonso-Fernandeza, M. C. Fairhurstb, J. Fierrez, and J. Ortega-Garcia, "Impact of signature legibility and signature type in off-line signature verification," in Biometrics Symposium 2007. IEEE, September 2007, pp. 1–6.

[5] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. FaundezZanuy, V. Espinosa, A. Satue, I. Hernaez, J. -J. Igarza, C. Vivaracho, D. Escudero, and Q. -I. Moro, "MCYT baseline corpus: a bimodal biometric database," Vision, Image and Signal Processing, IEE Proceedings -, vol. 150, no. 6, pp. 395–401, Dec 2003

[6] S. Pal, A. Alireza, U. Pal, and M. Blumenstein, "Multi-script off-line signature identification," in Hybrid Intelligent Systems (HIS), 2012 12th International Conference on, Dec 2012, pp. 236–240

[7] V. Nguyen, M. Blumenstein, and G. Leedham, "Global features for the off-line signature verification problem," in Proceedings of the 2009 10th International Conference on Document Analysis and Recognition, ser. ICDAR '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 1300–1304

[8] M. A. Ferrer, F. Vargas, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features." IEEE Transactions on Information Forensics and Security, vol. 7, pp. 966–977, 2012

[9] Porwik, P. and Doroz, R. (2014). Self-adaptive biometric classifier working on the reduced dataset, in M. Polycarpou et al. (Eds.), Hybrid Artificial Intelligence Systems, HAIS 2014, Lecture Notes in Computer Science, Vol. 8480, Springer, Cham, pp. 377–388

[10] M. A. Joshi, M. M. Goswami and H. H. Adesara, "Offline handwritten Signature Verification using low level stroke features," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 1214-1218, doi:10.1109/ICACCI. 2015. 7275778.

[11] A. Kumar and K. Bhatia, "k-NN based Writer Independent Offline Signature Verification System," 2021 International Conference on Technological Advancements and Innovations (ICTAI), 2021, pp. 612-616, doi:10.1109/ICTAI53825.2021.9673479.

[12] Kumar and K. Bhatia, "Artificial Neural Network based Writer-Independent Offline Signature Verification," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 704-707, doi:10.1109/ICIEM54221.2022.9853079.

[13] Hamadene and Y. Chibani, "One-Class Writer-Independent Offline Signature Verification Using Feature Dissimilarity Thresholding," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1226-1238, June 2016, doi:10.1109/TIFS.2016.2521611.

[14] P. Chaturvedi and A. Jain, "Feature Ensemble based method for verification of Offline Signature images," 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 2022, pp. 710-714, doi:10.1109/COM-IT-CON54601.2022.9850628.