# ijRASET

# INTERNATIONAL JOURNAL
# FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

www.ijraset.com

Call: ○ 08813907089     |     E-mail ID: ijraset@gmail.com

# A Comprehensive Survey of Digital Methods for Signature Verification

Tanuja Bhadarge

*Department of Applied Sciences, Parul University*

*Abstract: Signatures are considered a tool for identification in the case of bank statements, bank cheques, property papers, etc. So, signature forgery is commonly seen for personal gain or benefit. Examining a large number of manual documents can consume a lot of time and effort. Also, signatures provide us with a very small quantity of alphabets or content, so it is usually difficult to identify the characteristics. Consequently, there is a massive growth in the digital era in biometric personal verification and authentication systems, which are based on physical unique characteristics (DNA, fingerprints, hand geometry, face, or ear) or behavioral patterns (voice, etc.). Until now, various digital methods have been proposed for signature verification. In this paper, we present a comprehensive survey of signature verification systems. The topics related to handwriting identification, its other categories, and analysis problems are also described. The comparison of all the digital methods is shown on the basis of EER, FAR, FRR, accuracy, and time required.*
*Keywords: Signature verification, FAR, FRR, EER, digital methods, accuracy.*

## I. INTRODUCTION

Handwriting is a neuromuscular task that involves 30 bones and more than 40 muscles. It is an acquired skill. The timing and movements of the hand are different for every individual. That's why handwriting and signatures are considered unique characteristics of an individual. Document examination is a discipline that seeks to determine the history of a document through technical or scientific processes [1]. Albert S. Osborn is mainly credited with launching handwriting identification. Handwriting identification is a discriminatory process that is done by comparing writings. The examination of a document is conducted to determine the origin, the production process, and the source. The manual analysis of any writing is carried out in two steps: Firstly, the class characteristics of the writing are compared, which are the common characteristics (size, slant, alignment, etc.) of the writing. The second step includes individual characteristics (letter design, initial and terminal strokes, embellishments, etc.) that are unique to each writing. A survey was conducted in [12], in which the forensic document examiners were compared with the non-examiners. And the analysis report says that for document examination, expertise is required.

Signature forgery is seen in cases related to bank checks and legal documents. The main problem for forensic handwriting examination is the specializations of criminals [6]. The signatures are performed in different languages, which makes the analysis difficult. It takes a lot of time and effort to manually review a big number of documents. Therefore, in an effort to address this issue, researchers began developing several digital techniques for signature verification. There are two signature verification systems used:

1) Online signature verification system in which an electronic device such as a tablet or stylus is used, which also captures features such as pressure, speed, and direction. It is also considered a dynamic system.
2) Offline signature verification system in which the signatures are written offline, and then the system scans the image and stores the image.

Offline signature verification can be carried out using two different approaches. One approach is writer-dependent signature verification, where features are extracted from genuine and forged signatures for each writer. Then compare the test signature sample with its own training sample. The demerit of this approach is that the expert has to extract the features for each new writer. The second approach, writer-independent signature verification, is used by forensic examiners. This approach is thought to be the most practical since it is not necessary to extract features for each writer in order to verify the signature. In this case, general features are built from some writers chosen randomly. Automatic Signature Verification, the state of art paper, has shown various techniques, features, and verification processes used by different systems [29] [30].

This paper is organized as follows: Section II discusses different types of forgeries; Section III introduces the methodology followed for the signature verification system. Section IV introduces functioning estimation metrics; Section V introduces different methods of signature verification systems; Section VI gives a comparison of different digital methods and a discussion; and Section VII concludes the paper.

## II.    TYPES OF FORGERIES

The main task of a forensic expert is to detect whether the signature is genuine or forged. Forgery in the signature verification system is broadly classified into three parts. Fig. 1. represents the types of forgeries.

1) Random forgery: Forgeries that lack specific details regarding the signer's name and style are referred to as random forgeries.
2) Unskilled forgery: Unskilled forgeries are signatures in which the forger simply knows the signatory's name and lacks a previous sample.
3) Skilled forgery: signatures in which the forger is aware of the signatory's name and the original signature's style. Skilled forgeries are most difficult to identify.
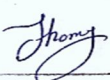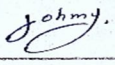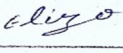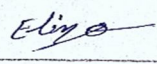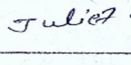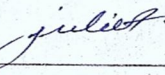


Fig. 1: Types of forgeries

## III.    METHODOLOGY FOLLOWED FOR SIGNATURE VERIFICATION

Most signature verification systems consist of four main steps: data acquisition, pre-processing, feature extraction, and verification. An overview of this is shown in Fig. 2.



Fig. 2: Overview of signature verification system.

### A.    Data Acquisition

Data for signature verification is obtained using scanners and cameras so that the data is present in digital format. In dynamic systems, the signatures are directly stored on the tablet.

### B.    Pre-processing

The treatment of the signatures obtained. In static signatures, typical pre-processing involves noise removal by filters, resizing, normalizing, thinning, and smearing. In dynamic signatures, pre-processing involves filtering, noise reduction, and smoothing.

### C.    Feature Extraction

The crucial step for signature verification. In the feature extraction step, the system extracts the characteristics from the given sample and records them in order to produce details in the form of observation data. The accuracy of the verification depends on the feature extraction. Feature extraction methods can be classified into two types: function features and parameter features.

1) *Function Features:* The signature is usually described in terms of a time function whose values comprise the feature set [29] . It includes position, velocity, acceleration, pressure, force, direction, etc.
2) *Parameter features:* The signature is described as a course of elements, each one representative of the value of a feature [29]. Furthermore, parameters can be further classified into two main categories:
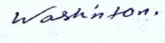a) Global features: It deals with the whole signature. It comprises the total signature time duration, the number of pen-ups and pen-downs, the number of components, etc.
b) Local features: It deals with features extracted from specific parts of the signature. It comprises the height-to-width ratio of the stroke, grid-based information, pixel density, texture, etc.

### D.  Verification

The extracted features are stored in a knowledge base. Any person's signature depends on several factors, including their characteristics and their mental and emotional condition. The criteria for verification are set on the basis of the variation of the features. For high-security applications like military, etc., a high value is used, while for other applications such as banking, a moderate value is used. After fixing the value, test samples are used to be matched to verify if a given signature is genuine or forged.

## IV.    FUNCTIONING ESTIMATION METRICS

A signature verification system's analysis report is determined by how well it can identify fake signatures. Several presentation valuation metrics are applied to many signature verification systems on the basis of which the estimation is made, and they are compared. These metrics contain false acceptance rate (FAR), false rejection rate (FRR), equal error rate (ERR), accuracy, and time required. False Acceptance Rate (FAR) is the number of times the system accepts a forged signature as the original signature. False Rejection Rate (FRR) is the number of times the system rejected the original signature. When the false acceptance rate (FAR) and false rejection rate (FRR) are equal in the system, then it is known as the equal error rate (EER). This is the point at which we can say that the system has equal chances of accepting and rejecting the forged and original signatures. After evaluation of the total samples (FAR, FRR, and EER), accuracy and time required are calculated.

## V.    METHODS FOR SIGNATURE VERIFICATION SYSTEM

Numerous computer-assisted systems, tools, software, or methods are used; a few of them are described below:

1) WANDA Workbench [9]: It is an open framework for electronic data processing. While a new system is developed, we should keep in mind that it should be followed for the next decade. So, to ensure long-term operations, WANDA works on two stable standards: the programming language Java and the data interchange language XML (eXtensible Markup Language). The fundamental processes that are followed in this system are: data acquisition (scanning, tablet input, combined); preprocessing (annotation of handwritten documents); measurement of selected handwriting characteristics; automatic feature extraction; and search in the data pool. Moreover, the WANDA workbench can be used and further developed in the future by adding more features and easy processing methods.

2) Genetic algorithm [10] : The proposed method is based on fuzzy logic and genetic algorithm methodologies. The method uses two stages: fuzzy inference system training using a genetic algorithm and signature verification. The training set includes genuine forgeries, random forgeries, and skilled forgeries. The features used in this system are projection profiles, contour profiles, geometric center, actual dimensions, signature area, local features, and baseline shift. The system has attained a signature recognition rate of 90%.

3) Support Vector Classifier Model [11] : In this model, two methods are used: SVM and the K-means algorithm. This model is trained for a real signature dataset and can detect forged signatures. Support vector machines can use kernels to do both linear and nonlinear classifications [11]. The K-means-means assists in obtaining the most similar signature image. The model is divided into four stages: data pre-processing (RGB to grayscale conversion; region of interest; thinning, etc.), feature extraction (contour features of the image; scale-invariant feature transform), model training, and model testing. This model has shown an accuracy of 95.83% for forgery detection.

4) Open-layered framework [12]: The main aim of this framework is to remove background noise signals and ensure no loss of parts of handwriting after preprocessing. In the other systems, the limitations were poor separation of handwriting from a textured background and poor threshold binarization. To conquer this problem, an open-layered framework was developed. This framework successfully works for textured background removal, homogenous background removal, reconstruction and noise removal, stamp and imprint removal, line removal, and stroke reconstruction. This framework was used by the Bundeskriminalamt, the federal police bureau in Germany, for one and a half years.

5) CEDAR-FOX software [13]: As a result of a USNIJ-sponsored study on handwriting individuality, an information processing model known as CEDAR-FOX software for handwriting examination was developed. This software contains several tools for interactive handwriting examination as well as methods for autonomous operation [13]. In autonomous mode, it can perform several methods, such as writer verification, writer identification, and signature matching. Several methods for comparing strings of binary feature vectors for handwritten characters are evaluated.

6) Fourier descriptor: distance measure [14]: The suggested method is based on Fourier transform and chain code features. Signature identification is divided into two stages: recognition and verification. In the recognition process, principle component analysis is used, and in the verification process, a multilayer feed-forward artificial neural network is used. Different distance measurements were used to analyse the results in the recognition system, and the Manhattan distance has shown good results.

7) Online signature verification using string matching [15]: String matching, also known as dynamic time wrapping, is a well-known method for comparing strings of different lengths. It aligns the points in two strings so that the total of the disparities between the aligned pairs is as small as possible. All alignments are investigated to find the minimum difference. Strings can also be connected if the strokes are broken. In this system, the signatures are acquired using a digitizing tablet. The input signature is compared with the stored reference set of the signature. The similarity of the input signature and the reference set of signatures is completed using string matching, and the similarity value is compared to a threshold.

8) Multiple algorithm method [16]: In this method, the ensemble of classifiers based on the graphometric features is used so as to reduce false acceptance and improve the reliability of the classification. An ensemble classifier's primary objective is to combine several classifiers in order to lower the misclassification rate of a poor classifier. The features used are distribution, curvature, density, and slant. After the comprehensive experiments, two different scenarios were demonstrated, demonstrating that ensembles based on graphometric features are quite efficient and can considerably reduce the false acceptance rate error.

9) Two-stage neural network classifier [17]: The system is based on three powerful feature sets in combination with a multiple-stage neural network-based classifier [17]. The system is divided into four steps: preprocessing (noise reduction, data area cropping, width normalization, and skeletonization), feature extraction (global features, texture features, and grid information), first-stage classification, and second-stage classification. The first-stage classifier is based on the use of three multi-layer perceptron's, one for each group of features. The first neural network, NN1, has 16 inputs; the second, NN2, has 96 inputs; and the third, NN3, has 48 inputs. The second classification is based on radial basis function neural networks, which combine the results of the first-stage classification and make the final decision about whether the signature belongs to the owner or not.

10) Graphology and Graphometry [18]: In this method, the features from graphology and graphometry are used, and the evaluation is done using hidden Markov models. Graphology is claimed to be useful for everything, such as understanding health issues, morality, and mental problems. The feature sets used in this method are: caliber, proportion, spacing, alignment to baseline, progression, pressure, gesture, occupation of the graphical space, minimal graphics, and slant. All these features are applied through experimentation using hidden Markov models, which have shown an average 10% error in results.

11) Pixel matching technique [19]: In this method, pixel matching is used for signature verification. It is done in two major phases. 1. Pre-processing 2. Verification. The pre-processing step includes capturing the signature, removing noise and colour, and adjusting the properties of the signature, such as angle, size, etc. Each step has a different algorithm. To adjust the image properly in the center, the algorithm has to be changed according to it. In the verification process, the signature is compared with the original signature.

12) Verification using a multi-network classifier [20]: The signature verification is based on global geometric features and wavelet-transformed features. The preprocessing of the signature is done, which includes linearly normalizing the gray level of each image, computing the histogram of the gray-level normalized image, setting a threshold at the level above which there are 65% of the total pixels, and assigning a pixel to 1 (black) if its gray level is greater than the threshold and to 0 (white) otherwise. The global features included the height and width of a signature image, the number of black pixels, the baseline shift of the signature image, etc. The wavelet transformation was used to build the multi-resolution representation for both signature images and their projections. The results indicate that the system could detect free-hand forgeries accurately and could also monitor simulated forgeries with accuracy.

13) Verification using the grid approach [20]: In this system, the structural information of the image was partially obtained based on a grid that was superimposed on the normalized signature image [20]. The images of the samples are compared at the grid level. The results indicate that this system can detect free-hand forgeries and can monitor simulated forgeries.

14) Multi-expert system for dynamic signatures [21]: The system is based on the segmentation technique of handwritten signatures. It provides compatible stroke-oriented descriptions of the test and the reference signatures and allows signature analysis by strokes. For the feature extraction phase, function features such as position, velocity, and acceleration domain with time are used. A graphic tablet was used for sample collection.

15) Verification using textural and allographic features [22]: He had developed a new technique for automatic writer identification and verification that uses probability distribution functions (PDFs), which are extracted from the handwriting images, to identify the writer. The system works on two levels: the texture level and the character-shape (allograph) level. The proposed system is applicable for free-style handwriting (both cursive and isolated).

16) HMM online signature verification [23]: In this model, a function-based approach is presented for online signature verification. A collection of time sequences and hidden Markov models are used by the system. HMMs were introduced in the pattern recognition field as a robust method to model the variability of discrete-time random signals where context information is available [23]. The features included are basic functions (horizontal and vertical position trajectories, pressure signal), geometric normalization, and extended functions (path tangent angle, path velocity magnitude, log curvature radius, and total acceleration magnitude). The MCYT bimodal biometric database was used, and analysis was performed.

17) HMM offline signature verification [24]: He developed an offline signature verification system that uses features that are based on the calculation of the radian transform (RT) of a signature image. For the experiment, we used feature vectors of dimension d = 512 and observation sequences of length N = 256. HMM has N = 64 states with one allotted forward link (l = 1). This system is compared with human verification, and the results show that it can be used as a substitute.

18) HMM with cross-validation [25]: The system used is based on HMM with cross-validation. The cross-validation principle is used to derive not only the best HM models but also an optimal acceptance/rejection decision threshold for each writer. The verification technique captures the unique qualities of signatures using basic features. To begin with, the signature image is divided into local square cells by a grid that is overlaid on it. From each cell, the pixel density is computed and considered as the associated local feature. The pixel density is calculated for each cell size and is regarded as the corresponding local feature. The k-means vector quantization algorithm converts the signature image into a series of real vectors, which are then converted into a series of discrete symbols. The system can detect random forgeries accurately and identify the actual writer.

19) Fuzzy Vault [26]: This system is based on cryptographic construction, providing encryption and decryption of secret data using a fuzzy key, which is an unordered set of points. E.g., if a person named Riya places a secret S in a vault using an unordered set (fuzzy key), another person, Diya, will only be able to reveal the secret if her unordered set B is similar to A. The first encoding process is done for a 128-bit secret 'S', and then a decoding process is performed, which at the end provides us with information on whether the secret is valid or not.

20) EDM: Geometric Center [27]: The proposed system uses a geometric center for feature extraction. The Euclidean distance model is used for classification. The threshold range is built on statistical structures like average and standard deviation. The geometric features are based on two sets of points in the 2D plane. Vertical splitting and horizontal splitting are the feature points used. The FAR of the system is 9.39%, and the FRR is 14.58%.

## VI.    COMPARISON AND DISCUSSION

The table below consists of different methods used for signature verification. The writers have described the efficiency of the systems in various forms. They had used different kinds of error rates depending on the sample set. The table consists of complete data from various systems with their error rates. For the system to be used, the error rate should be the lowest.

| Sr. no | Approach | FRR | FAR | Accuracy | Time Required | EER |
|---|---|---|---|---|---|---|
| 1 | Wanda Workbench | - | - | 92% | - | - |
| 2 | Genetic Algorithm | - | - | 73.50% | - | - |
| 3 | Support Vector Classifier Model | - | - | 95.83% | - | - |
| 4 | Open layered framework | - | - | - | 41 sec | - |
| 5 | Fourier descriptor - Distance measure | 1.60% | 2.60% | - | - | - |
| 6 | CEDAR -FOX Software | - | - | 98.71% | - | - |
| 7 | Online Signature Verification using string matching | 2.80% | 1.60% | - | - | - |
| 8 | Multiple algorithm method | - | - | - | - | 5.90% |
| 9 | Two stage neural network classifier | 9.80% | 3% | 80.80% | - | - |

| 10 | Graphology and Graphometry | 3.60% | 13.29% | - | - | - |
|----|----|----|----|----|----|----|
| 11 | Pixel matching technique | 0.12% | 0.12% | - | - | - |
| 12 | Verification using multi network classifier | 6.65% | 5.65% | - | - | - |
| 13 | Verification using grid approach | 5.35% | 8.65% | - | - | - |
| 14 | Multi-expert system for dynamic signature | 18% | 31% | - | - | 0.40% |
| 15 | Verification using textural and allographic features (Individual) | - | - | - | - | 10.20 % |
| 16 | HMM online signature verification | - | - | - | - | 0.43% |
| 17 | HMM offline signature verification | 9.00% | 10.50% | - | - | 12.60 % |
| 18 | HMM with cross validation | 0.96% | 0.41% | - | - | 0.68% |
| 19 | Fuzzy Vault | 57.30 % | 0.75% | - | - | - |
| 20 | EDM-Geometric centre | 14.58 % | 9.39% | - | - | - |

Though a lot of research is going on in this field, there are still challenges in this area. The signatures can be done in various languages and patterns, so making a database for these is not practically possible.

## VII.    CONCLUSION AND FUTURE WORK

In this paper, we have summarized the systems, software, or methods used for digital signature verification. There are many approaches used in this area, but accuracy in the case of skilled forgeries is still required. The accuracy of the existing system shows good results, but every system shows limitations. So, to minimize the error, additional research is needed in the signature verification system. In the future, the fusion of various classifiers can be used for verification results.

## REFERENCES

[1]  Harralson HH, Miller LS. Huber and Headrick's Handwriting Identification: Facts and Fundamentals. CRC press; 2017 Dec 14.
[2]  Franke K, Köppen M. A computer-based system to support forensic studies on handwritten documents. Int J Doc Anal Recogn. 2001;3:218-31.
[3]  Chatzisterkotis T. An examination of quantitative methods for Forensic Signature Analysis and the admissibility of signature verification system as legal evidence [Doctoral dissertation]. University of Kent (United Kingdom); 2015.
[4]  Black DA. Forged signatures more skillfully written than the true signatures. J Crim L Criminol Police Sci. 1962;53:109.
[5]  Araujo RSA, Cavalcanti GD, Carvalho Filho ECDB. On-line verification for signatures of different sizes. In: Tenth international workshop on frontiers in handwriting recognition. Suvisoft; 2006. p. 1-4.
[6]  Krasiuk IP. Problems of forensic handwriting examination in the analysis of signatures and short notes. Nauk Visnyk. 2022;27(1):72.
[7]  Fairhurst MC, Kaplani E, Guest RM. Complexity measures in handwritten signature verification. In: HCI. 2001. p. 305-9.
[8]  Manning KA, Srihari SN. Computer-assisted handwriting analysis: Interaction with legal issues in US courts. In: International Workshop on Computational Forensics. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. p. 137-49.
[9]  Franke KY, Schomaker LRB, Veenhuis C, Vuurpijl LG, Erp MV, Guyon I. WANDA: A common ground for forensic handwriting examination and writer identification.
[10] Jayasekara B, Jayasiri A, Udawatta L. An evolving signature recognition system. In: First international conference on industrial and information systems. IEEE; 2006. p. 529-34.
[11] Anagha R, Kumar C. Signature recognition and forgery detection. Authorea Preprints. 2023.
[12] Franke K, Köppen M. A computer-based system to support forensic studies on handwritten documents. Int J Doc Anal Recogn. 2001;3:218-31.
[13] Leedham SSG, Srihari S. A survey of computer methods in forensic handwritten document examination. In: Proceeding the Eleventh International Graphonomics Society Conference. Scottsdale, Arizona; 2003. p. 278-81.
[14] Ismail IA, Ramadan MA, El-Danaf TS, Samak AH. An efficient off-line signature identification method based on fourier descriptor and chain codes. Int J Comput Sci Netw Secur. 2010;10(5):29-35.
[15] Jain AK, Griess FD, Connell SD. On-line signature verification. Pattern Recognit. 2002;35(12):2963-72.
[16] Bertolini D, Oliveira LS, Justino E, Sabourin R. Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognit. 2010;43(1):387-96.
[17] Baltzakis H, Papamarkos N. A new signature verification technique based on a two-stage neural network classifier. Eng Appl Artif Intell. 2001;14(1):95-103.
[18] Oliveira LS, Justino E, Freitas C, Sabourin R. The graphology applied to signature verification. In: 12th conference of the international graphonomics society. 2005. p. 286-90.

[19] Bhattacharya I, Ghosh P, Biswas S. Offline signature verification using pixel matching technique. Procedia Technol. 2013;10:970-7.

[20] Qi Y, Hunt BR. A multiresolution approach to computer verification of handwritten signatures. IEEE Trans Image Process. 1995;4(6):870-4.

[21] Bovino L, Impedovo S, Pirlo G, Sarcinella L. Multi-Expert Verification of Hand-Written Signatures. In: ICDAR. 2003. Vol. 3, p. 932-6.

[22] Bulacu M, Schomaker L. Text-independent writer identification and verification using textural and allographic features. IEEE Trans Pattern Anal Mach Intell. 2007;29(4):701-17.

[23] Fierrez J, Ortega-Garcia J, Ramos D, Gonzalez-Rodriguez J. HMM-based on-line signature verification: Feature extraction and signature modeling. Pattern Recognit Lett. 2007;28(16):2325-33.

[24] Coetzer J, Herbst BM, Du Preez JA. Off-line signature verification: A comparison between human and machine performance. In: Tenth International Workshop on Frontiers in Handwriting Recognition. Suvisoft; 2006.

[25] El-Yacoubi A, Justino EJR, Sabourin R, Bortolozzi F. Off-line signature verification using HMMs and cross-validation. In: Neural Networks for Signal Processing X. IEEE Signal Processing Society Workshop; 2000. Vol. 2, p. 859-68.

[26] Freire-Santos M, Fierrez-Aguilar J, Ortega-Garcia J. Cryptographic key generation using handwritten signature. In: Biometric technology for human identification III. SPIE; 2006. Vol. 6202, p. 225-31.

[27] Majhi B, Reddy YS, Babu DP. Novel features for off-line signature verification. Int J Comput Commun Control. 2006;1(1):17-24.

[28] Gonzalez-Rodriguez J, Fierrez-Aguilar J, Ramos-Castro D, Ortega-Garcia J. Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems. Forensic Sci Int. 2005;155(2-3):126-40.

[29] Impedovo D, Pirlo G. Automatic signature verification: The state of the art. IEEE Trans Syst Man Cybern C Appl Rev. 2008;38(5):609-35.

[30] Dimauro G, Impedovo S, Lucchese MG, Modugno R, Pirlo G. Recent advancements in automatic signature verification. In: Ninth International Workshop on Frontiers in Handwriting Recognition. IEEE; 2004. p. 179-84.

[31] Morales A, Morocho D, Fierrez J, Vera-Rodriguez R. Signature authentication based on human intervention: performance and complementarity with automatic systems. IET Biom. 2017;6(4):307-15.

[32] Chalechale A, Naghdy G, Premaratne P, Mertins A. Document image analysis and verification using cursive signature. In: 2004 IEEE International Conference on Multimedia and Expo (ICME). IEEE; 2004. Vol. 2, p. 887-90.

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ◯ (24*7 Support on Whatsapp)