Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

An integrated approach on verification of signatures using multiple classifiers (SVM and Decision Tree): A multi-classification approach

Upasna Jindal [1], Surjeet Dalal [1, *], G. Rajesh [2], Najm Us Sama [3], N. Z. Jhanjhi [4], Mamoona Humayun [5]

[1]Department of CSE, SRM University, Delhi-NCR, Sonipat, Haryana, India
[2]Department of IT, MIT Campus, Anna University, Chennai, Tamil Nadu, India
[3]Department of Science, Deanship of Common First Year, Jouf University, Sakaka, Saudi Arabia
[4]School of Computer Science and Engineering, SCE, Taylors University, Jaya, Malaysia
[5]Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakakah, Saudi Arabia

ARTICLE INFO

Article history:
Received 17 November 2020
Received in revised form
11 February 2021
Accepted 15 November 2021

Keywords:
Online
Offline
Feature extraction
Database
Classifiers
Local and global

ABSTRACT

A signature is a handwritten representation that is commonly used to validate and recognize the writer individually. An automated verification system is mandatory to verify the identity. The signature essentially displays a variety of dynamics and the static characteristics differ with time and place. Many scientists have already found different algorithms to boost the signature verification system function extraction point. The paper is aimed at multiplying two different ways to solve the problem in digital, manual, or some other means of verifying signatures. The various characteristics of the signature were found through the most adequately implemented methods of machine learning (support vector and decision tree). In addition, the characteristics were listed after measuring the effects. An experiment was performed in various language databases. More precision was obtained from the feature.

1. Introduction

A signature is a graphical depiction of the writer's name, giving the one way to identify the person's authentication. Human signature is based on behavioral and physical characteristics which are further fall into two categories: Online signature and offline signatures. Both the signatures are different from each other in terms of the way to signing and sequence of features contains.

1.1. Digital signature vs handwritten signature

Online, signatures are taken using a digitizer having a stylus, and dynamic features are captured while writing in space provider to the person (Kiani et al., 2009). In comparison, offline signatures are quite different, collected using pen paper, open space given to the signer, and features collected are static in nature. Considering previous research on the system, online signatures are more accurate than offline (Swain et al., 2020; Saeed et al., 2020). One major factor which affects the total performance is noise. Higher the noise lowers down performance. In other terms, the performance of the verification system depends on the factor of noise available in the input signatures. The key objective of the signature verification system (SVS) is to discriminate the human signatures into the defined classes either genuine/original or forged. Every time when the person signs there are certain variations that come in that, due to some stress, environmental conditions ad any other physical trait. This term can be called Inter/Intra personal variations.

- Forgery classification

Further forgery is also having some classes such as Random, Skilled, and Unskilled depending upon the presentation (Kiani et al., 2009):

- Random: Where signer knows the presentation of signature.
- Skilled: Where signer knows name and representation of the signature.
- Unskilled: Where signer does not know name and signature.
- Signature verification system (Guru and Prakash, 2008; Vargas et al., 2009; Jarad et al., 2014)

* Corresponding Author.
Email Address: profsurjeetdalal@gmail.com (S. Dalal)

https://doi.org/10.21833/ijaas.2022.01.012
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-4325-9237
2313-626X/© 2021 The Authors. Published by IASE.

In this system, the signature image is normalized and checks whether the image matches the original image or not. For security purposes, SVS can be used, such as verification for assessing entry applications and password substitutions. Signature verification has four stages namely acquisition and preprocessing, feature extraction, classification, and verification. Signature verification system block diagram given in Fig. 1.

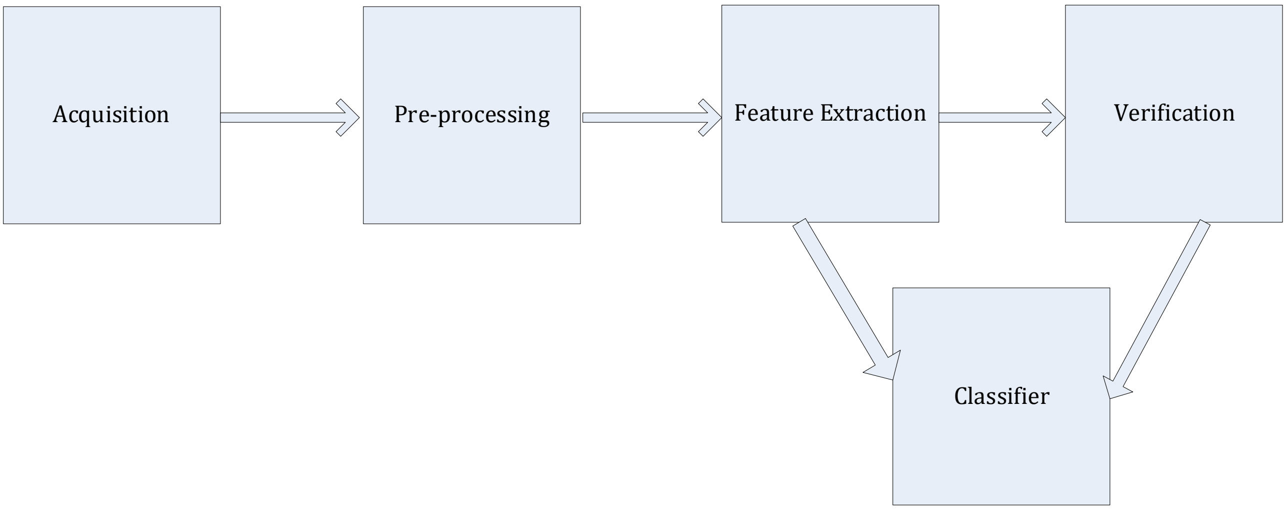


Fig. 1: Signature verification system

- Phases and their description in the signature verification system

Step 1: Signature images collected via a pen-paper or any digital device. Pre-processing phase makes the signature image prepared for the next phase i.e., feature extraction. This stage also includes binarization, rotation, scaling, thinning, cropping, and many others. Fig. 2 explains the steps involved in the pre-processing. How signature image becomes clean and clear for next step.

Step 2: Feature Extraction: This section is the main part of the signature verification. It is called as respiratory of the system, where features are classifieds into two local and global, both the classes have their own set of features, which needs to extract while calculating the forgery factor from the signature image. Local and global features are their sub-division is described in the below Fig. 3.

Step 3: Classification: Classification plays a vital role in the verification process, where the signature image is trained using single or multiple classifiers. Most of the researchers have given different learning approaches to train the input. Some of the classifiers which are used for the process are listed below in Fig. 4.

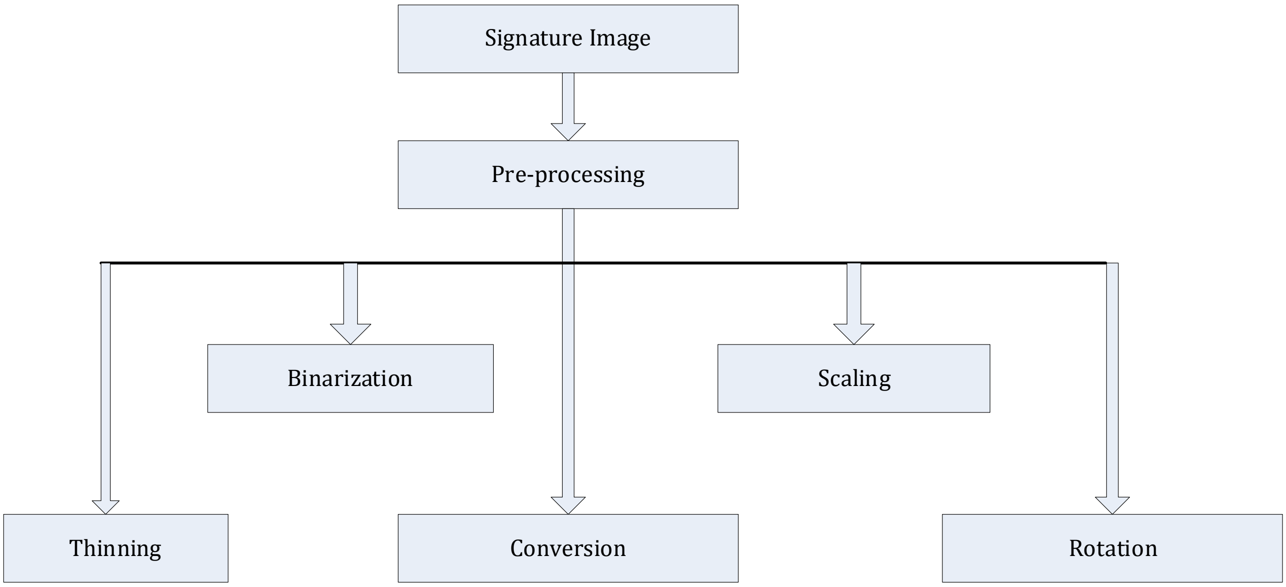


Fig. 2: Pre-processing phase

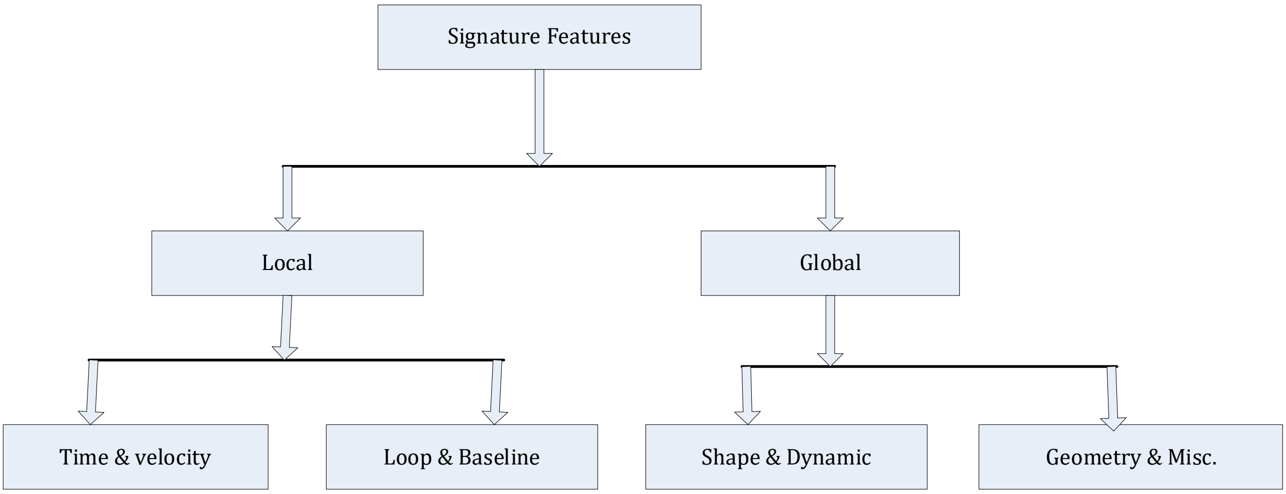


Fig. 3: Classification of local and global features

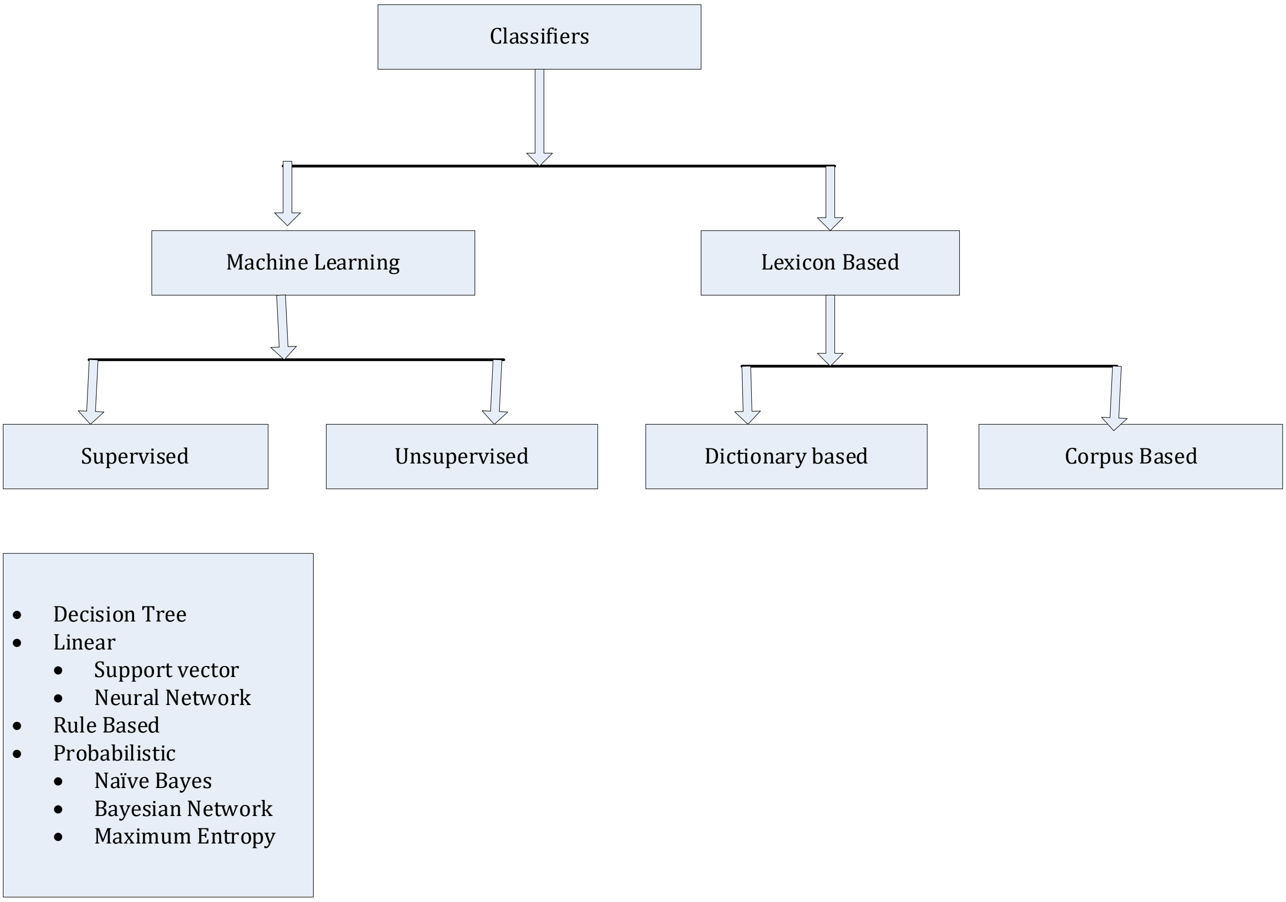


Fig. 4: Represents the types of classifiers

Step 4: Verification: In this step, a certain decision comes in the form of scores, which are further matched with the original score of the signature. It is accomplished by some distance measure and decision rules e.g., Euclidean distance, Mahalanobis measure, etc. Previously authors have calculated the False Acceptance Rate (FAR), False rejection rate (FRR), Equal error rate (EER), and other terms as result. The formula for calculating the distance is mentioned below:

1. Euclidean Distance: Defines the average distance between the two points of signature.

Consider two images I, J where points in the images are:

I={I_1, I_2, I_3... I_n}nd J = {J_1, J_2, J_3, J_n}
D= $\sqrt{\sum_{m=1}^{n}(Im-Jm)^2}$.

2. Mahabalonis Distance: To calculate the covariance between two feature vectors and maintain the matrix (Qiao et al., 2011).

M= $\frac{1}{n}\sum_{i=1}^{n}\left((xi-m)\middle|(xi-n)^T\right)$.

M is the mean value, i is the input image, n be the set of signature images.

3. Decision Score: Calculating the score where

Score (S; ID)= $\sum_{m=1}^{M}\left(F\left(X(Ref\ S_{IDm},\ S)\right)\middle|Meann_{ID};\partial\right)$

M is the set of signatures; Ref S is the reference signature trained using classifiers.

The above three measures support the process to find out the forgery factory from signatures.

2. Research motivation

Our main aim is to develop a secure system that helps us to find the forged signature out of a set of signatures, whether offline or online, and the main challenge is a skilled forgery, where chances of forgery are very high as compared to others. Signatures are broadly classified into global, local, and transitional features. Global features describe the entire signature including length, width, height, etc. whereas local features consider small of signature and extract detailed information from it. Verification of the system depends on two steps: Extraction and classification. More extraction, better classification will produce a high rate of accuracy and increase performance.

2.1. Classifiers used to calculate forgery factor using different datasets of offline and online signature

Based on the previous approaches, Table 1 shows that the features extracted, their classifiers used to find out forgery and accuracy obtained. Most of the researchers have used already available data of signatures and created their own set. An experiment was done on various datasets of signatures. Some of the authors used their own data set.

Table 1: Summary of existing work done

Author, Type, Year	Classifiers	Dataset	Accuracy
Oliveira et al. (2007) offline	Hidden Markov Models	60 writers included 30 training signatures, 10 casual forgeries, 10 original, and 10 skilled forged	FAR 2.83% FRR 2.50%, 1.44%, and 22.67% was obtained for casual, random, and skilled forgeries
Abuhaiba (2007) Offline/Online	Graph Matching Problem	100 genuine	26.7% of EER achieved for Skill forgeries and 5.6% EER for random forgeries
Quan and Liu (2007) Online	HMM/ANN using time delay NN, Local time function position, and pressure	MCYT-100 signature includes 100 signers, 25 genuine and 25 forgeries	EER:=0.12%
Jena et al. (2008) Offline	60 features using Euclidean distance	16 originals and 24 Forgeries	FRR: 14.58% achieved
Kamel et al. (2008) Online	Singular Value Decomposition (SVD) numerical tool	dataset of 100 signatures, contains 20 genuine signatures	EER achieved is less than 2.37% from the previous
Yanikoglu and Kholmatov (2009) Online	Fast Fourier Transform (FFT), Pen up duration	SUSIG-Visual subcorpus, MCYT-100	Equal Error 6.2% and 12.1% on skilled forgeries
Soleymanpour et al. (2010) Offline	SVM using counter let transform, Directional features	10 genuine signatures skilled forgery (Persian, Turkish)	Error 4.5%
Qiao et al. (2011) Online	Dynamic time warping (DTW), Mahabalonis Distance, positions, pressure, azimuth, angle, and inclination angle	MCYT-100 biometric database	Equal error rate 5.23%
Sreeraj and Idicula (2011) Offline/Online	Likelihood ratios and applied methods used by Forensic Handwriting Examiners (FHEs)	SVC 2004, Bio Secure, SigComp 2009 (Chinese and Dutch)	Accuracy: 90% Dutch signatures
Kour et al. (2011) Online	Genetic Algorithm-Support Vector Machine (GA-SVM), Time function features	SVC 2004	Accuracy 83%
Kruthi and Shet (2014) Offline/Online	Global Features, SVM	Own dataset 336 Signatures with different pens	Accuracy 72.2 %
Bharadwaja (2015) Offline/Online	Global features, Euclidean Distance with a global threshold	30 original signatures and 35 forged (online and offline)	FAR in offline 11.4% FAR online 8.57%
Zulkarnain et al. (2015) Offline	Global Features added new features, Hipotenuse distance, SVM	GPDS-960 Total of 23049 genuine and 28800 forgeries signatures	Accuracy: 87.5%
Cpałka et al. (2016) Offline	initial, middle, and final time moments, DTW	MCYT-100, Bio Secure	FAR: 3.36% FRR: 3.33%
Lai et al. (2017) Online	Features related to scaling, rotation, length normalized	SVC-2004, MCYT-100 100 persons, with 25 genuine and random forgeries respectively	EER: 2.37%
Sharif et al. (2018) Offline	Global: aspect ratio, area of signature, pure width, pure height, and normalized actual signature height. Local: centroid, slope, angle, and distance	CEDAR, MCYT, and GPDS synthetic.	AER: 5G: 6.67% 10G: 5.96% 12G: 5.0%
Maergner et al. (2019) Offline	Key point graphs with approximated graph edit distance and ink-ball models	GPDS 100	EER: 4.17% FAR: 3.94%

3. Proposed work

The objective of our research is to design a robust integrated signature verification system. We have already studied different types of forgeries present in online and offline signatures. For this, a database containing skill level forgeries has been used. However, the proposed system will try to identify unique features from the signatures of a person. Thus deliberate or fake inputs may cause lower down verification rates. By using a support vector machine we can produce a better classification. The one major disadvantage of the SVM classifier is that more the input slows down the results.

To overcome the complexity of SVM, an addition of decision tree function produced better results previously, the hybrid SVM model was proposed embed C4.5 algorithm of a decision tree into the SVM and resulting in a more accurate and efficient hybrid classifier. Then we introduced the modified DT-SVM (Maergner et al., 2019; Blankers et al., 2009) algorithm addition of a new method, Probability-based Distance as Spitting Criterion, in which we use the distances in the frequency distribution of the instances. Thus, the modified DT-SVM provides better performance over the previous decision tree, and SVM (Ferrer et al., 2005) in comparison with the Computational Complexity and overall Accuracy. We have emphasized reducing input space using new splitting criteria. The proposed algorithm will show better performance from previous research.

i. Input signature: The input signatures are collected from persons where each signature has its own x-y coordinates, which are calculated from the pen up and pen down points. Every single point has is stored in the database. Representation of the signature can be done in the form of conservative coordinates i.e., x-y coordinates. Coordinates will be saved in the system in the .txt file Database for online and offline signatures are separate. Fig. 5 depicts the illustration of our proposed system i.e., integrated signature verification Fig. 5.

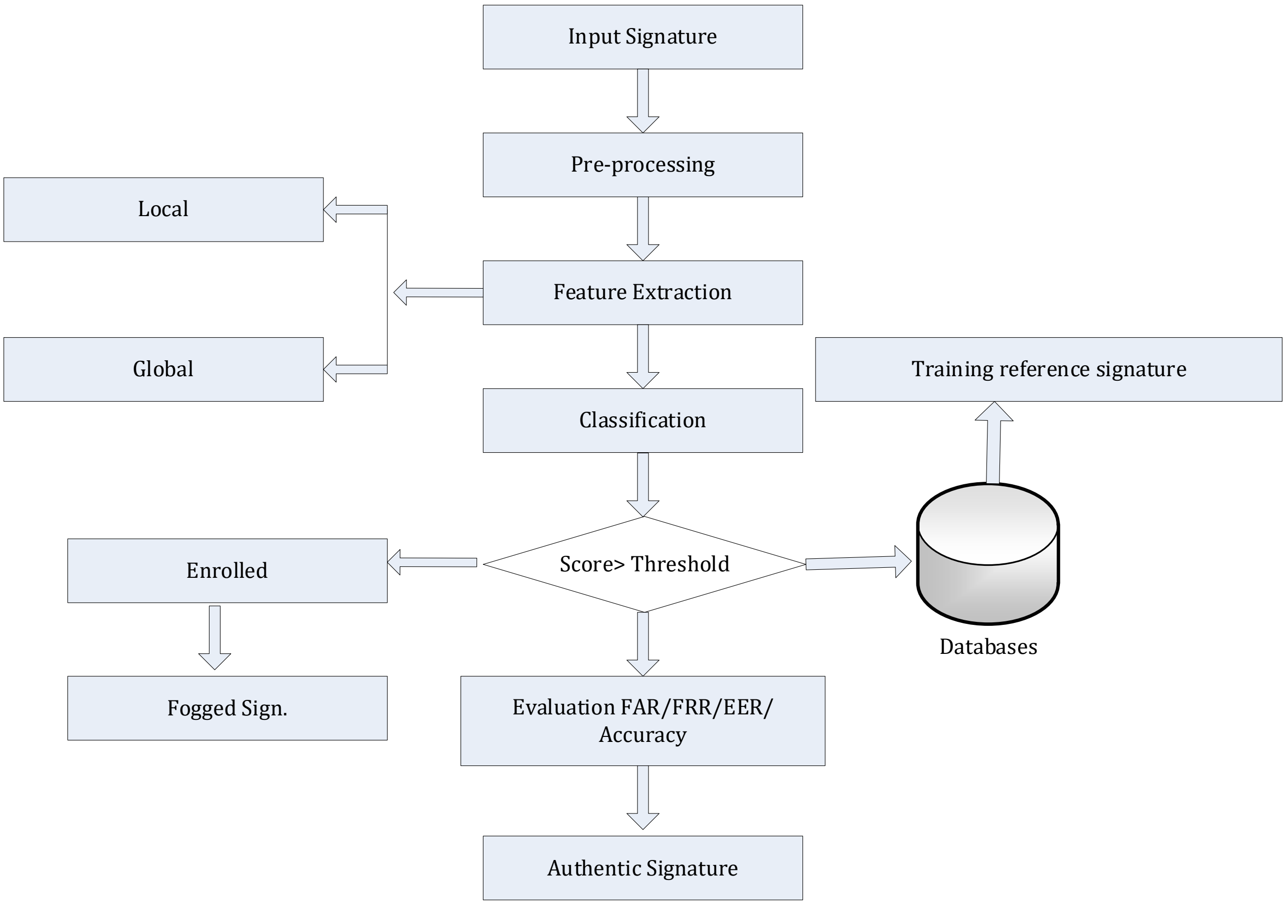


Fig. 5: Graphical illustration of the proposed system (ISV)

ii. Mathematical formulation: Signature Sample. Let $\lambda=\lambda\ (i)$ Where $\lambda \subset ¥$ be an input signature. $¥^{(g)}$ is the no. of genuine signature, $¥^{(f)}$ is the no. of a forged signature. $\{\lambda_i{}^{(g)} + \lambda_j{}^{(f)} \subset \lambda\}$, where i, j be the location of the pixels of the input signature.

$$i = [1,2,3 \ldots . n], \tag{1}$$
$$j = [1,2,3,4 \ldots \ldots m] \tag{2}$$

The output of the signature image is produced in terms of the forgery factory. The input signature is initially scaled and calculate length L s, and, find its velocity vector V^{new} directly comparable with each sample signature $\lambda(i)$, rotate in a clockwise direction to produce new velocity vector $V^{new}\ \lambda(i)$ having initial direction $V^{new}\ \lambda_{(i+j)}$. An indication that the new signature is forged (Bharadwaja, 2015) is then provided by large values of the ‘forgery index’:

$$\lambda^{\text{new}}=\frac{1}{\Pi l}\min[i=1..n,j=1..m]\int_0^l angle\,\text{Vnew}\,(\text{þ}\ {}_{\lambda(\text{i})(\text{t})},\lambda(\text{i})(\text{t}),\text{dt}, \tag{3}$$

Forgery Index then normalized (λ^{new}) to range lies either 0 or 1, and we assume it, to be small for original input signatures. In terms of λ^{new} theory testing, is a test statistic, for the null hypothesis that the new signature is original.

iii. Pre-processing: Pre-processing (Sheng et al., 2005) is another important phase of the verification system, to improve the overall accuracy and reduce the computational needs of the feature extraction phase. The main purpose of this phase is to make the standardized form of signature and prepare for the next phase i.e., feature extraction. It primarily includes the following steps Noise, conversion, resizing, thinning, normalization, transformation, and smoothing. All these are to avoid the developed system falsifying the original signature.

Size normalization is done by scaling each character, each node, and every point of direction both horizontally and vertically.

$$x_i=\frac{x_i^0-x_{min}}{x_{max}-x_{min}}W \tag{4}$$
$$y_i=\frac{y_i^0-y_{min}}{y_{max}-y_{min}}H \tag{5}$$

where x_i and y_i denote the point of original signatures is the corresponding point after the transformation:

$$x_{min}=\min i\,\{x_i^0\},x_{max}=\max i\,(x_i^0) \tag{6}$$
$$y_{min}=\min i\,\{y_i^0\},y_{max}=\max i\,(y_i^0) \tag{7}$$

where W and H are the width and height of the normalized signature respectively.

The re-sampling step SΔ is a fraction of the total arc length L. Below equations shows data points in the signature.

$$d_i=\sqrt{(x_i-x_{i+1})2+(y_i-y_{i+1})2} \tag{8}$$
$$L=\textstyle\sum_{i-1}^{n-1}d_i \tag{9}$$
$$\Delta S=\frac{L}{n_1} \tag{10}$$

Noise Removal: Given Fig. 6 is the example of a signature taken from the database for the pre-processing. For noise removal, a modified canny edge algorithm is defined, where the Sobel detection operator is used to detect the edges of the image (Mathur et al., 2016; Gao et al., 2010; Sheng et al., 2005; Vincent and Folorunso, 2009). As in the canny edge used Gaussian filter, which loses informational edges only isolated edges appeared. In our system, both the static and dynamic are available in the signature. To improve the edge detection modified canny edge algorithm was used. Step 1: An input signatures I, where I≥0. Step 2: Convert image I (grayscale image) into I_b i.e binary image, Step 3: Morphological operation on I_b, (If I_b <0,) then go to step 1 Else Step 4: After a normalized operation, I_b converts to I_n , Image is normalized, Step 5: Apply noise removal Canny edge using Sobel filter (Shokhan, 2014), Step 6: Calculate the Error from I_b. Step 7: Conversion of image I_b to image I_{new}.

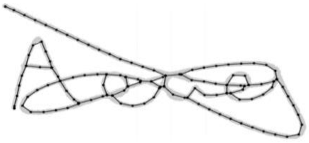


Fig. 6: Example showing the signature generated from database for the preprocessing

iv. Feature extraction: Feature extraction technique (Sharif et al., 2018) is respiratory of the verification process, and different extract attributes and characteristics from the given image and create a matrix for further purpose. Feature Extraction is broadly divided into three main categories: Global, Local and Geometrical.

Further, our system has two phases: Training and Testing. In the training phase, we applied a support vector machine and then classified the image. Output is displayed in the form of a feature matrix. In the testing phase, we applied a modified SVM-DT algorithm which is the proposed algorithm. For Decision function mapping with support vector machine (Shao et al., 2013; Zuo and Jia, 2016; Boonchuay et al., 2017; Nazari and Kang, 2015) where F(I) represents the decision function of the new signature image. K belongs to the I, Ix coordinates i.e., the kernel function to define the feature matrix.

$$F(i)=\textstyle\sum_{i=1}^{m}\propto\gamma iK(I,I_x)+B \tag{11}$$

The split function is used to calculate the feature space where cur_value denotes the current value of the features extracted from the original and forged signature.

if cur_value>Split Criteria then
return $\sqrt{\text{SplitCriteria}}$

Distances in features of the signature need to be calculated using the Frequency distributions function which is used to map the balance between unbalanced and balanced datasets of signatures.

The previously defined Bhattacharyya Coefficient is given below (Zuo and Jia, 2016).

P1 and P2 define the probability distribution distance of two signatures:

$$P(P_1,\ P_2)=\ \int_\Omega^0\sqrt{\frac{dP_1}{dv}\ .\ \ \frac{dP_2}{dv}\ dv\,.} \tag{12}$$

Derived distance using Bhattacharyya Coefficient in Eq. 13:

$$h_H(P_1,\ P_2)=$$

$$2\left[1-\ \int_{\Omega}^{0}\sqrt{\frac{dP_1}{dv}\ .\ \ \frac{dP_2}{dv}}\ dv\right]=\sqrt{\int_{\Omega}^{0}\left(\sqrt{\frac{dP_1}{dv}}-\ \sqrt{\frac{dP_2}{dv}}\right)^2 dv.} \qquad (13)$$

While integrating two classifiers, problems raise in their mapping because we have both balanced and unbalanced data. For mapping these data, we add The Bhattacharyya coefficient in the proposed algorithm using Probability-based Distance as Spitting Criterion.

4. Implementation and result analysis

In our research, two different experiments were carried out. One for the testing phase and the other training phase. The first experiment was conducted on the training phase of the system where signature features are extracted. The second experiment is applied in the testing phase using the proposed algorithm SVM-DT features of captured signature data. A performance evaluation is done for each phase. The proposed integrated signature verification system includes a database of original signatures which contains all the information of the features. The set of features are captured at the time of feature extraction further it will compare with the set of features of the forged signatures to verify the status of the signature. For comparison of such feature set, we propose an algorithm that has multiple classifiers Support Vector Machine and Decision Tree (SVM-DT) are applied. Given Fig. 7 shows some sample signatures collected from the dataset.

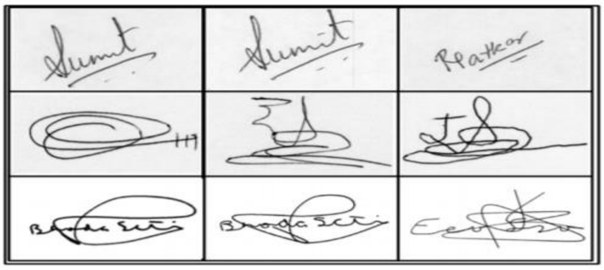


Fig. 7: Sample signature set for the verification purpose

In this system, set of total 1036 signatures we have taken. Out of these, 192 were trained and 47 were tested using the proposed algorithm DT-SVM. Using the proposed algorithm, the system displayed the false acceptance rate and false rejection rate for both global and local features. The results are very promising and decrease the rate of forgery. The verification results of the SVM and DT-SVM methods are given in Table 2. Fig. 8 shows **a** graphical representation of the implementation of the verification system and Fig. 9 shows the confusion matrix of the integrated signature verification system.

Table 2: Comparisons of results from the existing method

Classifiers	Dataset	Features extracted	FAR and FRR	Accuracy
Support vector Machine	336 Set signatures	Global	-	72.2%
GA- Support vector Machine (Kour et al., 2011)	SCV 2004	Time function features	-	83%
DTW (Cpałka et al., 2016)	MCYT, Biosecure	Initial, Middle, and final Time moments	FAR 3.33% FRR 3.36 %	-
Proposed Algorithm	192 Set signatures	Global and Local	FAR 3.40% FRR 2.28%	96.6%

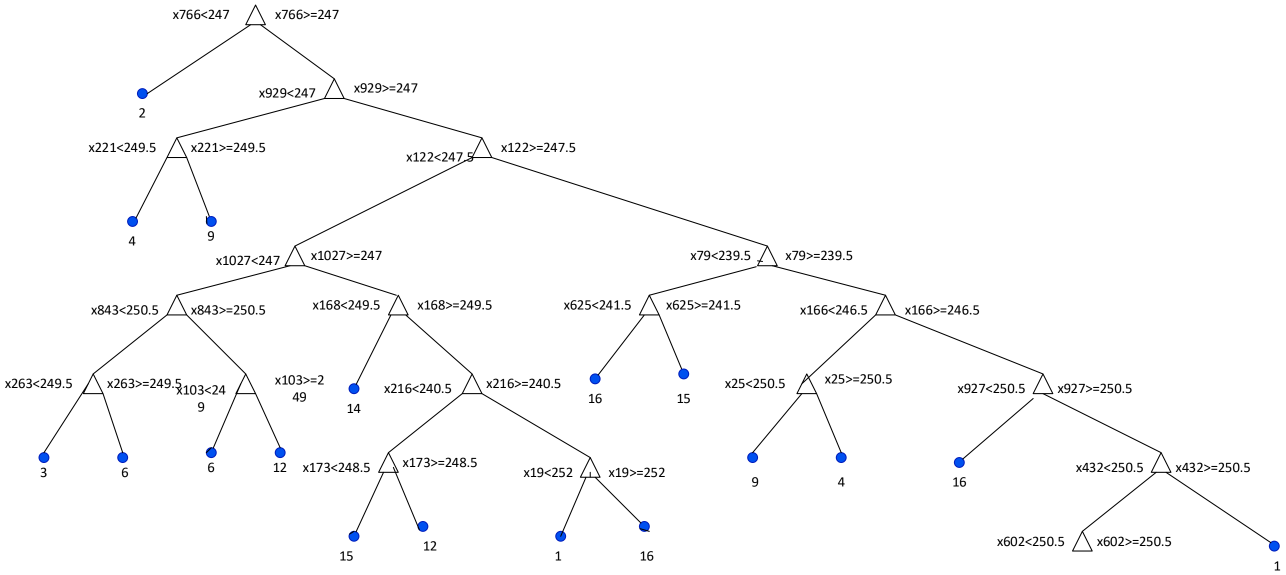
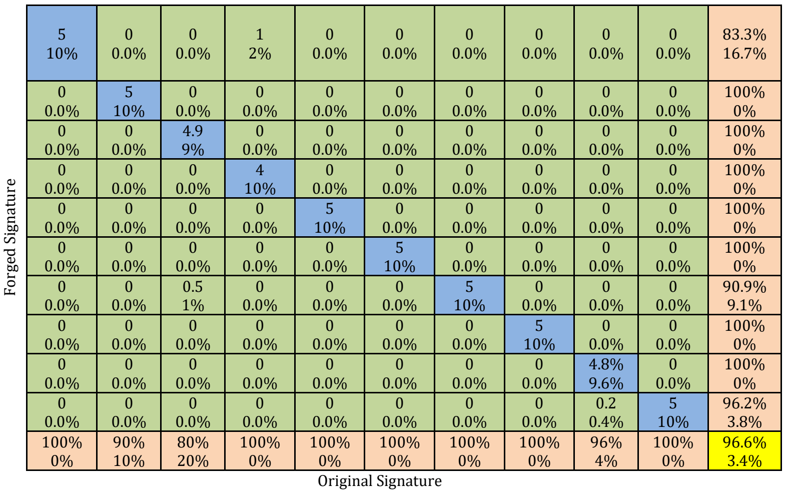


Fig. 8: Graphical representation of the implementation of the verification system



Forged Signature

5 10%	0 0.0%	0 0.0%	1 2%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	83.3% 16.7%
0 0.0%	5 10%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	4.9 9%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0 0.0%	4 10%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0.5 1%	0 0.0%	0 0.0%	0 0.0%	5 10%	0 0.0%	0 0.0%	0 0.0%	90.9% 9.1%
0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	5 10%	0 0.0%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	4.8% 9.6%	0 0.0%	100% 0%
0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0.2 0.4%	5 10%	96.2% 3.8%
100% 0%	90% 10%	80% 20%	100% 0%	100% 0%	100% 0%	100% 0%	100% 0%	96% 4%	100% 0%	96.6% 3.4%

Original Signature

Fig. 9: Confusion matrix of the integrated signature verification system

The Fig. 9 matrix is generated from the visualization of the proposed work. Each row and column are representing the forged class and original signature of the person.

4.1. Characteristics of performance analysis

In this section, we have calculated certain True positive, False Negative, and precision values of the signature dataset which is implemented on two different datasets of the training and testing phase (Tables 3 and 4).

4.2. ROC curve

In the integrated signature verification, we have plotted the receiver operating characteristics curve to illustrate the performance of our proposed system. It is the graphical representation of the results where x and y axis will represent the true positive rate and false positive rate respectively. In the given curve, there are three different signature sets represented in different classes 1, class 1, and class 2. Figs. 10, 11, and 12 of the ROC curve are generated at different threshold values.

Table 3: Characteristics of the training dataset

Class represent	True Positive	False Negative	Precision	F-Measures
Original Signatures	0.983	0.540	0.915	0.998
Forged Signatures	1.0	0.016	0.998	0.979
Weighted	0.965	0.008	0.953	0.973

Table 4: Characteristics of the testing dataset

Class represent	True Positive	False Negative	Precision	F-Measures	
Original Signatures	0.999		0.512	0.943	0.996
Forged Signatures	1.0		0.023	0.988	0.996
Weighted	0.989		0.058	0.996	0.998

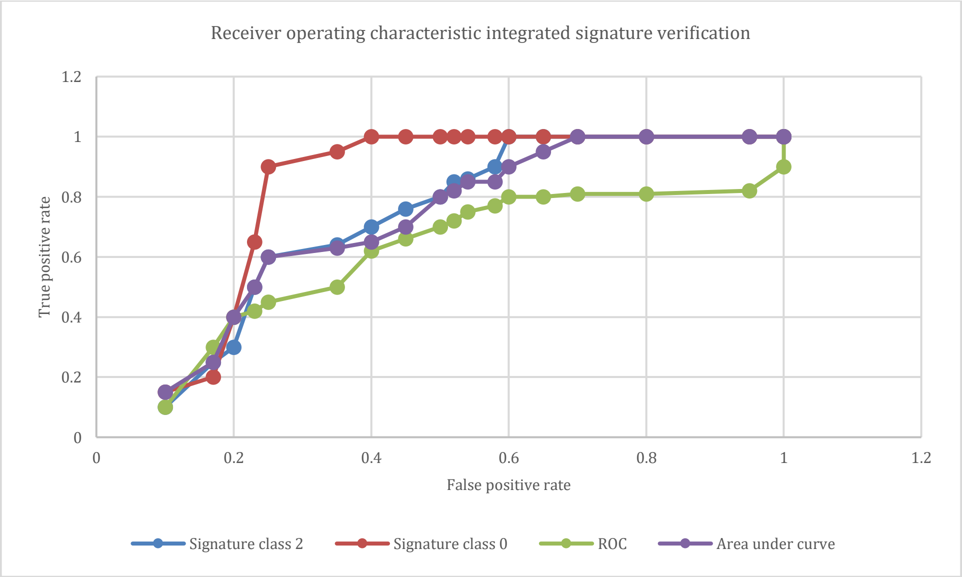


Fig. 10: ROC curve @ threshold value=0.5

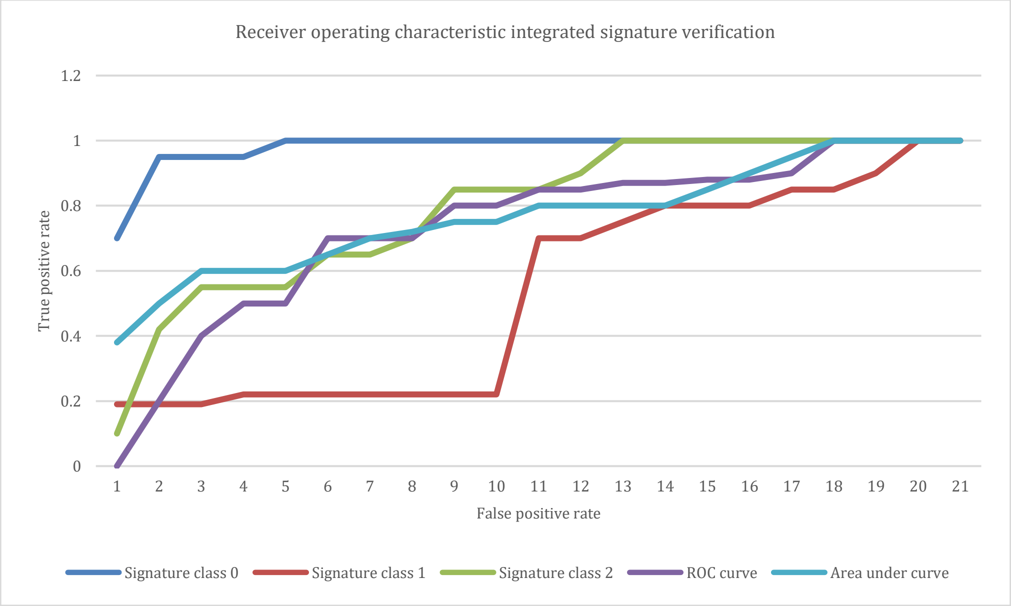


Fig. 11: ROC curve @ threshold value=0.25

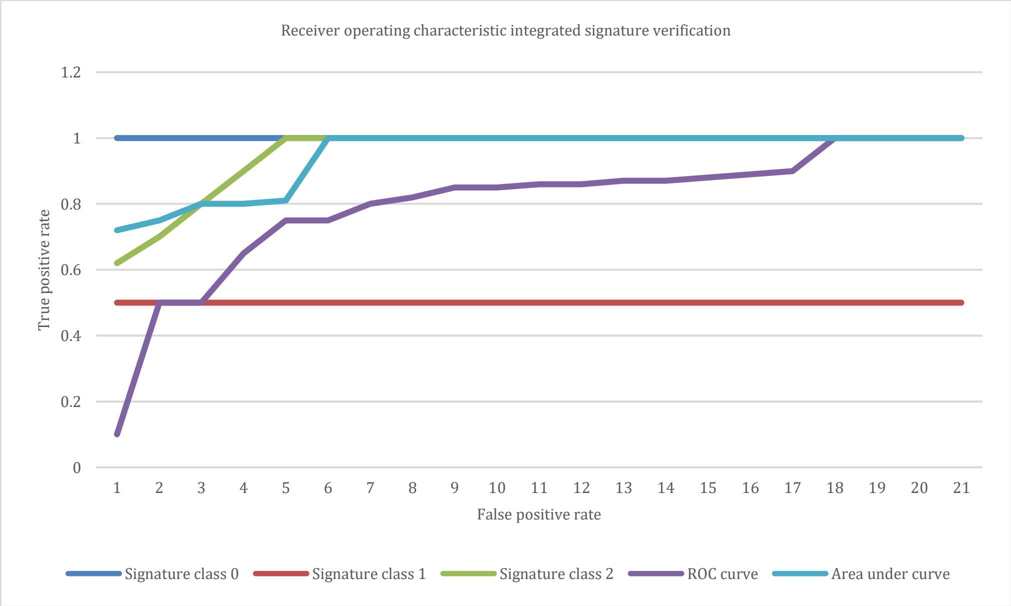


Fig. 12: ROC curve @ threshold value=0.05

In the end, it is clear that combining two classifiers gives better and more accurate results and reliability than the previously used classifiers. The main of our research is to show the reduction in the error rate from the signature image and find out the forgery rate from the signature. From the above section 5, certain scores of the signature have been generated. Experiment analysis is done using the machine learning tool.

5. Results

As expected, the Accuracy results of the integrated systems are much better than previous systems. The accuracy achieved 96.6%. Use of single classifiers, the systems are not able to compute within the variability of a person. Generally expected to yield better results when presented with more classifiers for the reference signatures.

6. Conclusion and future scope

This paper presents a brief survey of various features and methods for the classification of the set features from the signature image. These approaches are studied according to their different stages, and the performance evaluation based on FRR, and FAR is given. In addition, they can be analyzed for efficiency to get a better result. There is a need to develop one general system in future work to classify every style of signature and to enhance performance.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abuhaiba IS (2007). Offline signature verification using graph matching. Turkish Journal of Electrical Engineering and Computer Sciences, 15(1): 89-104.

Bharadwaja AV (2015). The analysis of online and offline signature verification techniques to counter forgery. Indian Journal of Science and Technology, 8(20): 1-7. https://doi.org/10.17485/ijst/2015/v8i20/77735

Blankers VL, van den Heuvel CE, Franke KY, and Vuurpijl LG (2009). Icdar 2009 signature verification competition. In the 10th International Conference on Document Analysis and Recognition, IEEE, Barcelona, Spain: 1403-1407. https://doi.org/10.1109/ICDAR.2009.216

Boonchuay K, Sinapiromsaran K, and Lursinsap C (2017). Decision tree induction based on minority entropy for the class imbalance problem. Pattern Analysis and Applications, 20(3): 769-782. https://doi.org/10.1007/s10044-016-0533-3

Cpałka K, Zalasiński M, and Rutkowski L (2016). A new algorithm for identity verification based on the analysis of a handwritten dynamic signature. Applied Soft Computing, 43: 47-56. https://doi.org/10.1016/j.asoc.2016.02.017

Ferrer MA, Alonso JB, and Travieso CM (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(6): 993-997. https://doi.org/10.1109/TPAMI.2005.125 **PMid:15943430**

Gao W, Zhang X, Yang L, and Liu H (2010). An improved Sobel edge detection. In the 3rd International Conference on Computer Science and Information Technology, IEEE, Chengdu, China, 5: 67-71. https://doi.org/10.1109/ICCSIT.2010.5563693

Guru DS and Prakash HN (2008). Online signature verification and recognition: An approach based on symbolic representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 31(6): 1059-1073. https://doi.org/10.1109/TPAMI.2008.302 **PMid:19372610**

Jarad M, Al-Najdawi N, and Tedmori S (2014). Offline handwritten signature verification system using a supervised neural network approach. In the 6th International Conference on Computer Science and Information Technology, IEEE, Amman, Jordan: 189-195. https://doi.org/10.1109/CSIT.2014.6805999

Jena D, Majhi B, Panigrahy SK, and Jena SK (2008). Improved offline signature verification scheme using feature point extraction method. In the 7th IEEE International Conference on Cognitive Informatics, IEEE, Stanford, USA: 475-480. https://doi.org/10.1109/COGINF.2008.4639204

Kamel NS, Sayeed S, and Ellis GA (2008). Glove-based approach to online signature verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 30(6): 1109-1113. https://doi.org/10.1109/TPAMI.2008.32 **PMid:18421114**

Kiani V, Pourreza R, and Pourreza HR (2009). Offline signature verification using local Radon transform and support vector machines. International Journal of Image Processing, 3(5): 184-194.

Kour J, Hanmandlu M, and Ansari AQ (2011). Online signature verification using GA-SVM. In the International Conference on Image Information Processing, IEEE, Shimla, India: 1-4. https://doi.org/10.1109/ICIIP.2011.6108923

Kruthi C and Shet DC (2014). Offline signature verification using support vector machine. In the Fifth International Conference on Signal and Image Processing, IEEE, Bangalore, India: 3-8. https://doi.org/10.1109/ICSIP.2014.5

Lai S, Jin L, and Yang W (2017). Online signature verification using recurrent neural network and length-normalized path signature descriptor. In the 14th IAPR International Conference on Document Analysis and Recognition, IEEE, Kyoto, Japan, 1: 400-405. https://doi.org/10.1109/ICDAR.2017.73 **PMCid:PMC5337438**

Maergner P, Howe NR, Riesen K, Ingold R, and Fischer A (2019). Graph-based offline signature verification. Available online at: https://arxiv.org/abs/1906.10401

Mathur N, Mathur S, and Mathur D (2016). A novel approach to improve Sobel edge detector. Procedia Computer Science, 93: 431-438. https://doi.org/10.1016/j.procs.2016.07.230

Nazari Z and Kang D (2015). Density based support vector machines for classification. International Journal of Advanced Research in Artificial Intelligence, 4(4): 69-76. https://doi.org/10.14569/IJARAI.2015.040411

Oliveira LS, Justino E, and Sabourin R (2007). Off-line signature verification using writer-independent approach. In the International Joint Conference on Neural Networks, IEEE, Orlando, USA: 2539-2544. https://doi.org/10.1109/IJCNN.2007.4371358

Qiao Y, Wang X, and Xu C (2011). Learning Mahalanobis distance for DTW based online signature verification. In the IEEE International Conference on Information and Automation, IEEE, Shenzhen, China: 333-338. https://doi.org/10.1109/ICINFA.2011.5949012 **PMid:21861052**

Quan ZH and Liu KH (2007). Online signature verification based on the hybrid hmm/ann model. International Journal of Computer Science and Network Security, 7(3): 313-322.

Saeed S, Abdullah A, Jhanjhi NZ, Naqvi M, and Humayun M (2020). Performance analysis of machine learning algorithm for healthcare tools with high dimension segmentation. In: Agrawal R, Chatterjee JM, Kumar A, Rathore PS, and Le DN (Eds.), Machine learning for healthcare: Handling and managing data: 115-128. CRC Press, Boca Raton, USA. https://doi.org/10.1201/9780429330131-9

Shao YH, Chen WJ, Huang WB, Yang ZM, and Deng NY (2013). The best separating decision tree twin support vector machine for multi-class classification. Procedia Computer Science, 17: 1032-1038. https://doi.org/10.1016/j.procs.2013.05.131

Sharif M, Khan MA, Faisal M, Yasmin M, and Fernandes SL (2018). A framework for offline signature verification system: Best features selection approach. Pattern Recognition Letters, 139: 50-59. https://doi.org/10.1016/j.patrec.2018.01.021

Sheng Y, Phoha VV, and Rovnyak SM (2005). A parallel decision tree-based method for user authentication based on keystroke patterns. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 35(4): 826-833. https://doi.org/10.1109/TSMCB.2005.846648 **PMid:16128463**

Soleymanpour E, Rajae B, and Pourreza HR (2010). Offline handwritten signature identification and verification using contourlet transform and Support Vector Machine. In the 6th Iranian Conference on Machine Vision and Image Processing, IEEE, Isfahan, Iran: 1-6. https://doi.org/10.1109/IranianMVIP.2010.5941179

Sreeraj M and Idicula SM (2011). A survey on writer identification schemes. International Journal of Computer Applications, 26: 23-33. https://doi.org/10.5120/3075-4205

Swain M, Kisan S, Chatterjee JM, Supramaniam M, Mohanty SN, Jhanjhi NZ, and Abdullah A (2020). Hybridized machine learning based fractal analysis techniques for breast cancer classification. International Journal of Advanced Computer Science and Applications, 11(10): 179-184. https://doi.org/10.14569/IJACSA.2020.0111024

Vargas JF, Ferrer MA, Travieso CM, and Alonso JB (2009). Offline signature verification based on pseudo-cepstral coefficients. In the 10th International Conference on Document Analysis and Recognition, IEEE, Barcelona, Spain: 126-130. https://doi.org/10.1109/ICDAR.2009.68

Vincent OR and Folorunso O (2009). A descriptive algorithm for sobel image edge detection. In the Informing Science and IT

Education Conference, Informing Science Institute, Macon, USA, 40: 97-107. https://doi.org/10.28945/3351

Yanikoglu B and Kholmatov A (2009). Online signature verification using Fourier descriptors. EURASIP Journal on Advances in Signal Processing: 260516. https://doi.org/10.1155/2009/260516

Zulkarnain Z, Rahim MSM, and Othman NZS (2015). Feature selection method for offline signature verification. Journal Technology, 75(4). https://doi.org/10.11113/jt.v75.5070

Zuo J and Jia P (2016). Proof on decision tree algorithm. Revista Técnica de la Facultad de Ingeniería Universidad del Zulia, 39: 276-280. https://doi.org/10.21311/001.39.7.34