Neural Computing and Applications
https://doi.org/10.1007/s00521-019-04220-x

ORIGINAL ARTICLE

Signature verification approach using fusion of hybrid texture features

Ankan Kumar Bhunia[1] · Alireza Alaei[2] · Partha Pratim Roy[3]

Received: 20 February 2018 / Accepted: 25 April 2019

Abstract
In this paper, a writer-dependent signature verification method is proposed. Two different types of texture features, namely discrete wavelet and local quantized patterns (LQP) features, are employed to extract two kinds of transform and statistical-based information from signature images. For each writer, two separate signature models, corresponding to each set of LQP and wavelet features, using one-class support vector machines (SVMs) are created to obtain two different authenticity scores for a given signature. Finally, a score-level classifier fusion based on the average method is performed to integrate the scores obtained from the two one-class SVMs and achieve the final verification score. To train the one-class SVMs in the proposed system, only genuine signatures are considered. The proposed signature verification method was tested using four different publicly available datasets to demonstrate the generality of the proposed method. The evaluation results indicate that the proposed system outperforms other existing systems in the literature.

Keywords Offline signature verification · Texture features · Wavelet transform · Local phase quantization · Score-level fusion

1 Introduction

Human physiological or behavioural characteristics, biometrics, are commonly used for person identification/authentication in day-to-day life. Handwritten signature, as a unique human personal characteristic, is an accepted means of person authentication. However, the manual handling of a large number of signatures generated everyday is cumbersome. It demands an automatic algorithmic approach to deal with the problem of person verification based on handwritten signatures [1–6]. As a result, many automatic methods were developed in the literature to deal with the problem of signature-based person authentication in various applications including person identification and verification, crime detection, bank cheque fraud detection, etc. [2–6]. A signature verification method generally distinguishes between a person's original and forged signatures, accepting the original signatures and rejecting the forged ones. Three different types of forgeries, namely random, simple, and skilled, were defined in the signature verification literature [1]. The skilled forgeries are generated by individuals who try to mimic an original signature and create one as close as possible to the original signature. Random and simple forgery samples are generated by individuals without any knowledge about the signers and their signatures. In other words, a random forgery is a genuine signature written by a different signer, whereas a simple forgery is a signature written by a different signer than original signer by looking at a genuine signature without any practice and prior knowledge about the signature. Indeed, the problem of signature verification considering skilled forgeries is more challenging compared to simple and random forgeries [1, 2].

Considering the type of information used for authentication, signature verification methods in the literature are categorized into: online and offline approaches. Online signature verification models use dynamic information, such as velocity, acceleration, pressure, stroke order, and force, whereas in offline systems, signature images are the static source of information. Therefore, the offline signature verification is comparably more challenging with respect to the online signature verification problem [1, 7].

✉ Partha Pratim Roy
proy.fcs@iitr.ac.in

[1] Department of EE, Jadavpur University, Kolkata, India

[2] School of Business and Tourism, Southern Cross University, Gold Coast, Australia

[3] Department of CSE, Indian Institute of Technology Roorkee, Roorkee, India

Published online: 06 May 2019

In the past, support vector machine (SVM) has been found to be well suited for signature recognition [8, 9]. Mainly, binary-class SVM (B-SVM) was used for modelling handwritten signature images [9]. In B-SVM-based signature verification methods, it is required to have both genuine and forged signatures for training. However, in practice, only genuine signatures are available. Moreover, local phase quantization (LPQ) and wavelet transform features were shown their high discrimination property in biometric analysis [10, 11]. In this work, a novel writer-dependent offline signature verification model based on one-class SVM classifiers and two different texture features, LPQ and wavelet, is proposed. These two different texture-based feature extraction methods are considered to better characterize handwritten signatures by extracting two types of information (statistical and transformed) from signature images. For each person's signature, two separate one-class SVM models are trained considering LPQ and wavelet texture features extracted from only genuine signatures. The scores obtained from the two one-class SVMs are then fused to verify the originality of test signatures. The reasons for choosing two one-class SVM classifiers are twofolds: (1) a single classifier may not perform well when the nature of features extracted from signatures is different, and (2) finding a single classifier to perform well on different datasets is difficult. As in our proposed feature extraction methods two different types of features are extracted, using multiple classifiers with different feature sets can improve the performance of the system, Moreover, the performance of multiple classifiers with different features can on an average be better than all the classifiers used separately.

The main contributions of this work are as follows. First, a writer-dependent signature model by using one-class SVMs is proposed that takes into account only genuine signatures for training. Second, wavelet and local quantized patterns (LQP) features, as transform- and statistical-based texture features, are employed to interpret two kinds of signature characteristics. Third, a novel score-level classifier fusion method is employed to obtain final signature verification results. Finally, a number of experiments using four different datasets collected in different contexts and languages are performed to evaluate and also to demonstrate the generality and high performance of the proposed signature verification system.

The remainder of this paper is organized as follows. In Sect. 2, the background of the work is reviewed. The proposed method is illustrated in Sect. 3. Databases, evaluation metrics, experimental results, and comparative analysis are presented in Sect. 4. Finally, conclusions and future work are provided in Sect. 5.

2 A brief literature review

Signature verification methods in the literature follow a common pipeline composed of: (1) pre-processing, (2) feature extraction, (3) training a classifier or creating a knowledge-based model, and (4) verification steps [1, 3]. The pre-processing includes various tasks, such as signature extraction, noise reduction, image normalization, binarization, skew/slant correction, and skeletonization [3]. All or a combination of these tasks is generally employed on signature images in each method to prepare them for the next step, feature extraction.

Following the pre-processing step, a set of discriminant features from the pre-processed signature images is extracted to interpret different aspects of signatures for the verification purposes. In the literature of offline signature verification, different feature extraction techniques including geometric, connected component (CC), directional and gradient, mathematical transformations, profiles and shadow-code, texture information, and interest points were proposed [7, 8, 10, 12–26]. Based on the level of granularity, feature extraction methods are grouped into local [9, 10, 12–15, 17–35] and global [7–9, 12, 13, 18, 20, 29, 36–39] approaches.

In the third step, various methods were proposed in the literature of offline signature verification to create signature models by training a classifier or creating a knowledge-based model [2–6]. The created/trained models were then used to classify a test signature as genuine or forged one. The signature models are either writer-dependent or writer-independent. In a writer-dependent approach, a specific signature model is created for each individual by using a few number of genuine signatures and random forgeries. In a writer-independent approach, however, a single model is created for all the individuals. Hybrid models were also proposed for signature verification [2–6]. Both writer-dependent and writer-independent models can be designed using machine learning, and similarity-based approaches. Neural networks (NNs) [7, 14, 22, 32, 40], Bayes classifier [12], hidden Markov models (HMMs) [5, 9, 25, 27, 36], support vector machines (SVMs) [8–10, 17–21, 23, 26, 31, 32, 34, 38, 39], Gaussian mixture models (GMMs) [13], Gentle AdaBoost algorithm [30], and ensembles of classifiers [31], as machine learning approaches, were used for signature verification in the past. As similarity-based approaches, different fuzzy membership functions (Takagi–Sugeno, trapezoidal, and triangular) [30, 41–45], K-nearest neighbour (KNN), dynamic time warping, and point matching [12, 13, 15, 19, 22, 24, 27–29, 36, 37] were also been developed in the literature for signature verification. Moreover, symbolic representation-based approach was also employed for signature verification [21, 35, 46].

There are also many review papers in the literature to demonstrate the state-of-the-art methodological developments in the field of signature identification/verification [1–5]. A number of competitions were further organized to fairly evaluate the existing signature verification methods and report recent signature verification results and technological achievements [6, 16]. It is worth mentioning that the literature of offline signature verification is well established, and a significant progress was demonstrated in this area. However, the methods presented in the literature of offline signature verification have a number of limitations [35] as illustrated in Table 1. In addition to the limitations mentioned in Table 1, there are also some more challenges [3] in the area of offline signature verification that still attract many researchers to further investigate in this field. The general challenges can be listed as: (1) a low inter-class variability between every individual's genuine signatures and skilled forgeries, (2) a high intra-class variability in every individual's handwritten signatures compared to the other individual's biometrics, (3) a limited number of signatures for creating offline signature verification models, and (4) only genuine signatures available for creating offline signature verification models. Furthermore, we noted that only a few research works reported the use of hybrid features and score-level fusion for signature verification in the literature [30]. Therefore, the use of two different texture features (hybrid) and a score-level fusion technique for the verification of offline handwritten signatures is proposed in this research work.

3 Proposed method

The block diagram of the proposed system is given in Fig. 1. The proposed system is divided into four major steps: (a) pre-processing, (b) feature extraction, (c) one-class SVM classification, and (d) fusion scores rule. Each step of the proposed method is detailed in the following subsections.

3.1 Pre-processing

Due to some unavoidable variations, in terms of size, pen thickness, rotation, and translation, in the signatures written by an individual, it is necessary to pre-process the signature images. The initial pre-processing task is the binarization of signature images. The Otsu's algorithm is, therefore, applied, and an optimal threshold is calculated separating the white pixels and black pixels so that their inter-class variance is maximal [47]. A Gaussian filter is further used to eliminate the noises from the input signature images and enhance the quality of the images. Finally, signature images are cropped to make the features invariant to translation. The cropped images are then used for feature extraction. Figure 2 illustrates the different pre-processing tasks employed on an input signature image.

3.2 Feature extraction

In any pattern recognition problem, feature extraction is a crucial step. In our approach, two types of texture features: local phase quantization (LPQ) [48] and discrete wavelet transform features (DWT) [49] are considered as feature extraction methods to obtain statistical and transform information from a given signature image. LPQ is used for

Table 1 Overview of different signature verification methods and their limitations

Type/approach	Limitations
HMM-based methods	Perform poor when a small number of signatures are used for training, and the model needs to be retrain whenever a new signer is added to the system
NN-based methods	Need sufficient data for training and convergence, and the system needs to be retrained when the number of signature classes is changed
SVM-based methods	Need to determine a proper kernel and tune its parameters, and it is complex and needs extensive memory for large-scale tasks
GMM-based methods	Need to determine the best number of the Gaussian models for the system cannot be generalized and predict accurately when using new data
Bayesian-based methods	Need prior knowledge, and the posterior distributions are also influenced by the prior knowledge
Similarity-based methods	Need to find a suitable distance, and it is also sensitive to unrelated features as all features contribute equally to the similarity measure
Symbolic-based methods	Need diverse signature samples from every person to obtain an appropriate mean and standard deviation in order to construct a representative symbolic model for the person

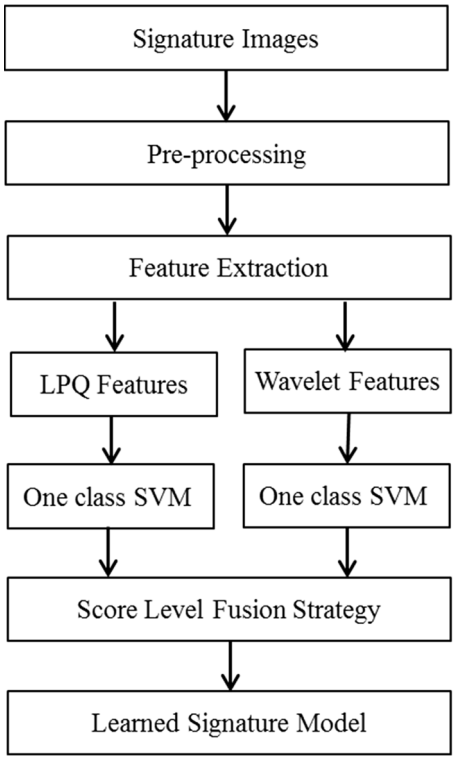

Fig. 1 Block diagram of our proposed signature verification method

feature extraction in our proposed method, as it is a spatial blurring method, which is able to represent all spectrum characteristics of an image in a very compact feature representation. Wavelet features alone were used for offline signature verification in the literature [10]. A key advantage of wavelet transforms compared to other transformation functions, such as Fourier transforms, is temporal resolution, which captures both frequency and location information, called location in time [49]. Therefore, wavelet transform-based feature is further used to be complementary to the statistical-based LPQ feature.

3.2.1 Local phase quantization

LPQ is a blur intensive texture feature extraction method [48]. The spatial blurring of an image ($g(x)$) can be represented by a 2D-convolution between the original image ($f(x)$) and a point spread function or PSF ($h(x)$), where the vector x represents the coordinate $[x_1, x_2]^T$. The spatial blurring of $f(x)$ can be expressed by a mathematical model [48] as follows:

$$g(x) = f(x) \otimes h(x) \tag{1}$$

In the frequency domain, the convolution becomes a product operation [48] described as:

$$G(u) = F(u) \cdot H(u) \tag{2}$$

where u is a frequency and $G(u)$, $F(u)$, and $H(u)$ are the discrete Fourier transforms (DFT) of the blurred image ($g(x)$), the original image ($f(x)$), and the PSF ($h(x)$), respectively. Furthermore, if we consider the phase of the spectrum, then the relation turns into a summation statement as $\angle G = \angle F + \angle H$.

The magnitude and phase can be separated into two forms as demonstrated in the following.

$$|G(u)| = |F(u)| \cdot |H(u)| \quad \text{and} \quad \angle G(u) = \angle F(u) + \angle H(u) \tag{3}$$

If $h(x)$ is centrally symmetric, i.e. $h(x) = h(-x)$, then H is always a real value, i.e. $\angle H \in \{0, \pi\}$.. For every pixel x from the image $f(x)$, the local spectra are computed using a short-term Fourier transform (STFT) in the local neighbourhood N_x as follows:

$$F(u,x) = \sum_{y} f(y)\omega_{\mathrm{R}}(y-x)e^{-j2\pi u^T y} \tag{4}$$

where $\omega_{\mathrm{R}}(x)$ is a rectangular window function [48].

The local Fourier coefficients are computed at four low frequency components: $u_1 = [a, 0]^T$, $u_2 = [0, a]^T$, $u_3 = [a, 0]^T$, $u_4 = [a, -a]^T$ where a is small enough to satisfy $H(u_i) \geq 0$. For each point x, we can write $F = [F(u_1, x), F(u_2, x), F(u_3, x), F(u_4, x)]$.

The phase information can be counted using a simple scalar quantization q_j.

$$q_j = \begin{cases} 1, & g_j \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

where g_j is the jth component of the vector $(x) = \mathrm{Re}\{F(x), \mathrm{Im}\{F(x)\}\}$. Then, the label image is defined as:

$$f_{\mathrm{LPQ}}(x) = \sum_{j=1}^{p} q_j(x)2^{j-1} \tag{6}$$

Fig. 2 **a** Original image, **b** image after binarization, and **c** image after filtering and cropping process

Finally, from Eq. (6), a histogram of 256-dimensional feature vector is created and considered as LPQ features [48] for each signature image in our experiments.

3.2.2 Wavelet features

The discrete wavelet transform (DWT) [49] is a powerful tool in signal processing. DWT transforms a signal $x(t)$ into a highly redundant signal of two variables: scale (j) and translation (k) as shown in the following

$$W_{\Psi}(j,k) = \int_{-\infty}^{+\infty} x(t)\psi^{*}_{j,k}(t)d \tag{7}$$

where $W_{\Psi}(j,k)$ represents the wavelet transform coefficient and ψ is the mother wavelet.

$$\psi_{j,k}(t) = \frac{1}{\sqrt{2^j}}\psi\left(\frac{t-k2^j}{2^j}\right) \tag{8}$$

The DWT of the signal x is then calculated by employing a low-pass and a high-pass filter simultaneously on the input signal (Fig. 3).

In the DWT tree presented in Fig. 3, H and L denote high-pass and low-pass filters, respectively. The symbol $\downarrow 2$ denotes sub-sampling. Outputs of the filters are given by the following equations

$$a_{j+1}[p] = \sum_{n=-\infty}^{\infty} l[n-2p]a_j[n] \tag{9}$$

$$d_{j+1}[p] = \sum_{n=-\infty}^{\infty} l[n-2p]d_j[n] \tag{10}$$

where a_j is used for the next step of the transform and d_j determines output of the transform. $l[n]$ and $h[n]$ are the coefficients of low-pass and high-pass filters, respectively.

In DWT, the input images are divided into four sub-bands, i.e. LL, LH, HL, and HH, where LL is the average component or approximation image and LH, HL, and HH are the three detail components. The LL sub-band can be decomposed again and thereby producing more sub-bands [49]. This process can be carried out in many levels. The features obtained from these approximation and detail sub-band images at different levels uniquely characterize textures. The statistical mean and standard deviation of the transformed image are computed as follows:

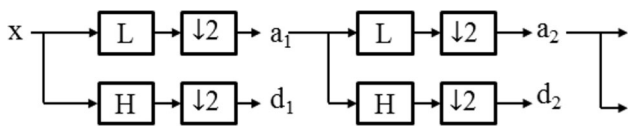

Fig. 3 Discrete wavelet transform (DWT) tree

$$\text{mean}(m) = \frac{1}{N^2}\sum_{x,y=1}^{N} w(x,y) \tag{11}$$

$$\text{Standard deviation}(S) = \left[\frac{1}{N^2}\sum_{x,y=1}^{N}(w(x,y)-m)^2\right]^2 \tag{12}$$

where $w(x,y)$ is the wavelet transform of the image at (x,y) and N is the size of the input image. The values calculated using Eqs. (11) and (12) are considered as the DWT features. As a result in our experiments, a feature vector of size 120 features is extracted from each signature image.

3.3 One-class SVM

Bi-class SVMs (B-SVM) have frequently been used to discriminate between genuine and forged signatures in the literature [9]. However, in a real scenario, only genuine signatures are available to train a signature verification system. Therefore, one-class SVM is a better choice compared to other classifiers, such as regression and neural networks, to handle a signature verification problem. One-class SVM is a special case of normal SVM that has been adapted to the one-class classification problem [50]. It separates all the data points in a feature space from the origin and maximizes the distance from the hyper-plane to the origin. The function returns + 1 in a small region near the training data points and − 1 otherwise. To separate the dataset from the origin, the following quadratic minimization function needs to be solved subjected to satisfying the other two conditions defined below

$$\begin{aligned} &\min_{w,\varepsilon_i,b} \frac{1}{2}w^2 + \frac{1}{\vartheta n}\sum_{i=1}^{n}\varepsilon_i - b \\ &(w\cdot \emptyset(x_i)) \geq b - \varepsilon_i \quad \text{and} \quad \varepsilon_i \geq 0; \quad \text{for all } i = 1,\ldots,n \end{aligned} \tag{13}$$

where ϑ is a tuning parameter. Due to the importance of this parameter, the one-class SVM is often called ϑ-SVM. If w and b solve this problem, then the decision function $f(x) = sign(w\cdot\emptyset(x) - b)$ will be positive for most examples x_i in the training set [50]. Each SVM includes a kernel function defined as $K(x,x') = \emptyset(x)^T\emptyset(x')$. Popular choices for the kernel functions are linear, polynomial, and sigmoidal of which radial base function (RBF) is the most used kernel function described as follows:

$$K(x,x') = \exp\left(-\frac{\|x-x\|^2}{2\sigma^2}\right) \tag{14}$$

where the $\sigma \in R$ is a kernel parameter.

By using a Lagrange technique and a kernel function, the decision function becomes:

$$f(x) = sign\left(\sum_{i=1}^{n} \alpha_i K(x, x') - b\right) \tag{15}$$

where n is the number of training data. The Lagrange multiplier α_i is computed by optimizing the following equations:

$$\min_{\alpha} \frac{1}{2} \sum_{i,j} \alpha_i \alpha_j K(x_i, x_j) \tag{16}$$

subjected to confirming following two equalities:

$$0 \leq \alpha_i \leq \frac{1}{\vartheta n} \tag{17}$$

$$\sum_{i}^{n} \alpha_i = 1 \tag{18}$$

In our signature verification framework, the features extracted from the LPQ and DWT are fed into two separate one-class SVMs. Based on the training data, two models for the genuine signatures of each user are formed. The two trained one-class SVMs (for each individual) provide two scores for a test signature. The two scores are finally combined, as explained in the following subsection, to get a single verification score for the given test signature.

3.4 Fusion rule for classification

Let T denote the target class for which we want to train our one-class SVM model and X represents an instance. The probability score of the instance X can be written as: $PS = P\left(\frac{T}{X}\right)$. A well-known and extensive approach for calculating the value $P\left(\frac{T}{X}\right)$ is to use a sigmoid function. Therefore, the probability score of a data point x of a particular class j is given by:

$$PS_j(x) = \text{sigmoid}\left(\sum_{i=1}^{n} \alpha_{ij} K(x, x') - b_j\right) \tag{19}$$

$$\text{sigmoid}(x) = \frac{1}{1 + e^{-x}}$$

As in our proposed model, two separate one-class SVMs (using two types of features: LPQ and wavelet) are trained for each signature class, and two probability scores $PS_j^{\text{LPQ}}(x)$ and $PS_j^{DWT}(x)$ are obtained for a signature x of the signature class j. Depend on the information obtained from different classifiers in an ensemble, there are different ways of combining the outputs of the classifiers. Based on the type of classifier outputs, information fusion methods at the decision level are categorized into three groups: (1) combining class labels, (2) class ranking, and (3) combining probabilistic outputs [51, 52]. As the outputs of our one-class SVM classifiers are probability values, a method from the third group is suitable for information fusion in our case. In the third group, called combining probabilistic outputs, there are various fusion strategies, such as average, sum, product, minimum, and maximum [53]. The average value of these two probability scores is considered to fuse the two classification probability scores and obtain a decision function $g_j(x)$, as it provides better verification results compared to the other fusion strategies, such as weighted average and maximum operator, in this group.

$$g_j(x) = \frac{\text{PS}_j^{\text{LPQ}}(x) + \text{PS}_j^{\text{DWT}}(x)}{2} \tag{20}$$

Finally, to classify genuine and forged signatures in the proposed model, the following decision rule is considered.

$$x = \begin{cases} \text{Genuine}, & \text{if } g_j(x) \geq T_j \\ \text{Forgery}, & \text{otherwise} \end{cases} \tag{21}$$

T_j is an acceptance threshold which is defined as:

$$T_j = m_j + k\sigma_j \tag{22}$$

where m_j and σ_j are the respective mean and standard deviation computed from the decision function during the training phase. Moreover, k is a control parameter, which is tuned during the training phase to obtain optimal results.

It is worth mentioning that feature fusion (concatenating the feature sets) could be performed to have only a single one-class SVM instead of two one-class SVMs to avoid score fusion step. However, experimental results shown in Sect. 4.2 demonstrate that score-level fusion strategy provides better results compared to feature-level fusion strategy.

4 Experimental results and discussion

4.1 Signature datasets and evaluation metrics

Four different offline signature databases, i.e. MCYT [54], GPDS-300 [45, 55], BHSig260 [56], and CEDAR [8], were used to evaluate the proposed signature verification method. The MCYT dataset is composed of 2250 signatures images collected from 75 signers and their associated skilled forgeries [54]. Each class contains 15 genuine signatures and 15 forgeries. Signatures were collected by using ink pens and paper [54].

The GPDS-300 dataset contains 16,200 offline signature images collected from 300 signers [45, 55]. Each signer has provided 24 genuine signatures. In each class of signatures, there are 30 skilled forged signatures obtained from ten different forgers. Generally, the first 160 classes of the GPDS dataset were used for testing and the last 140 classes were used for tuning and training the parameters.

Table 2 Examples of genuine and forged signatures from four different datasets

The BHSig260 dataset [56] contains 6240 genuine signatures and 7800 skilled forged signatures collected from 260 Indian native individuals of which 100 sets of signatures were written in Bengali and the rest, 160 sets, were written in Hindi. Similar to the GPDS-300 database, each class contains 24 genuine and 30 skilled forged signatures. The collected data were scanned using a flatbed scanner with the resolution of 300DPI in grey scale and stored in TIFF format.

The CEDAR dataset [8] is composed of signatures collected from 55 signers. Each signer has provided 24 genuine signatures and 24 forged signatures. Hence, the dataset contains 1320 (55×24) genuine signatures as well as 1320 forged signatures. To get an idea of signatures collected in each dataset, some samples of genuine and forged signatures from each dataset are shown in Table 2.

For evaluating the performances of our system, we considered three commonly used error metrics in the literature called false rejection rate (FRR), false acceptance rate (FAR), and average error rate (AER) [35].

4.2 Experimental setting and results

The proposed signature verification method in this research work is dependent on three parameters, i.e. the percentage of outliers (ϑ) and kernel parameter (σ) used in the one-class SVM and also acceptance parameter T. To obtain optimal results, various couples of (ϑ, σ) were considered during training the one-class SVMs using eight genuine signatures per user from the GPDS-140 dataset for training and the best couple ($\vartheta_{\text{opt}} = 0.01,\ \sigma_{\text{opt}} = 0.01$) was selected where the average error rate (AER) was the minimum. As the parameter T itself is dependent on the value k, the optimal values ϑ_{opt} and σ_{opt} were used to tune the parameter k. The parameter k was tuned in such a way that the FRR and FER became equal to obtain an equal error rate (EER). Theoretically, when the FRR and FER are equal, values considered for parameters, e.g. k, are optimal values. The FRR and FAR values obtained using different values of k for GPDS-140 dataset are plotted in Fig. 4. As can be seen from Fig. 4, EER was obtained when the value of k was set to 2.18.

To demonstrate the sensitivity of the results obtained from other dataset to the parameter k, we further calculated the parameter k for all other datasets. The values of k for each dataset (MCYT, BHSig260, and CEDAR) and their corresponding EER values obtained from the model considering eight genuine signatures per user for training and the rest (16) of the genuine signatures and 30 forgeries for tuning the parameters are illustrated in Table 3. From Table 3, we can note that the values of k for all the datasets are nearly the same. Thus, the proposed model is not sensitive to the parameter k on changing the dataset for training. As a results, in all the experiments on all the

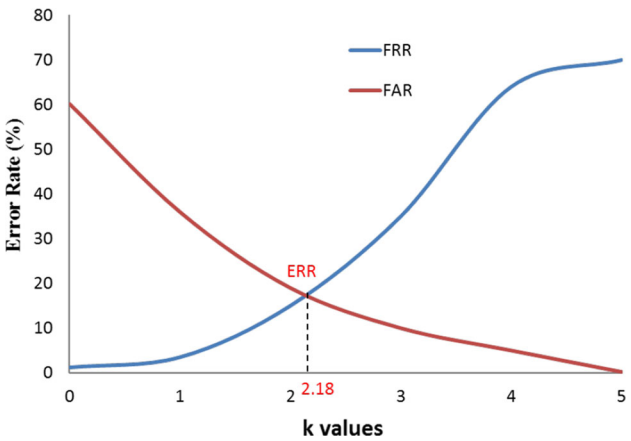

Fig. 4 FAR and FRR curves for different values of the parameter k on GPDS-140 dataset

Table 3 Results obtained from the proposed model using different k for different datasets

Datasets	GPDS-300	MCYT offline	BHSig-260	CEDAR
K	2.18	2.13	2.11	2.2
EER (%)	12.06	11.46	24.80	7.59

datasets, the value of k (= 2.18) obtained from the GPDS-140 was considered for testing the proposed system.

In our experiments, we used four offline handwritten signatures datasets, MCYT, GPDS-300, BHSig-260, and CEDAR. To evaluate our model, several experiments were carried out using different number of samples from the four datasets for training and testing the proposed model. In order to compare our results to those reported in the literature, we trained our model with 4, 6, 8, 10, 12, 14, and 16 genuine images per user. Table 4 represents different number of genuine signatures (N_g) and forgeries (N_f) used from each dataset in the design and evaluation steps of the proposed signature verification model. It is worth noting that the data samples used in design and evaluation steps are totally different and independent.

The error rates in terms of FRR, FAR, and AER obtained from the proposed signature verification model on the MCYT, GPDS, BHSig-260, and CEDAR datasets are shown in Table 5. As for each dataset, we have repeated ten times the training and the evaluation process with different randomly chosen signature samples, and the average of FAR, FRR, and AER is provided in Table 5. From Table 5, we can see that the AERs gradually decrease when the number of signatures for training increases in all datasets. The best result was obtained when 16 signatures used for training in each dataset. It can further be noted that even when the number of training signatures is less our model provides good results on the CEDAR dataset. It may

Table 5 Results obtained from the proposed model considering different datasets for evaluation

Dataset	Training		Testing		FAR (%)	FRR (%)	AER (%)
	N_g	N_f	N_g	N_f			
MCYT	4	0	11	15	18.12	20.11	19.12
	6		9		13.55	16	14.78
	8		7		11.77	12.1	11.94
	10		5		8.78	10.23	9.5
	12		3		8.00	9.13	8.57
	14		1		6.00	6.20	6.10
GPDS-160	4	0	20	30	17.89	18.12	18.01
	6		18		15.89	15.18	15.54
	8		16		12.56	11.56	12.06
	10		14		10.89	9.53	10.26
	12		12		8.56	7.5	8.03
	14		10		6.12	7.10	6.61
	16		8		4.12	4.24	4.18
BHSig-260	4	0	20	30	34.12	27.21	30.66
	6		18		27.12	26.12	26.62
	8		16		24.10	26.0	25.05
	10		14		20.1	24.18	22.14
	12		12		18.42	23.1	20.76
	14		10		14.30	15.13	14.72
	16		8		10.36	11.46	10.91
CEDAR	4	0	20	24	10.12	9.12	9.62
	6		18		8.2	8.4	8.3
	8		16		7.46	7.86	7.66
	10		14		6.12	7.2	6.66
	12		12		5.01	6.12	5.57
	14		10		3.56	4.18	3.87
	16		8		1.14	2.13	1.64

Table 4 Different number of samples used in design and evaluation steps

Database	#Writers	Training (samples per class)		Tuning the parameters (samples per class)	
		N_g	N_f	N_g	N_f
Design step					
GPDS-140	140	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	30
MCYT offline	40	14, 12, 10, 8, 6, 4	0	1, 3, 5, 7, 9, 11	15
BHSig-260	100	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	30
CEDAR	20	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	24
Evaluation step					
GPDS-160	160	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	30
MCYT offline	35	14, 12, 10, 8, 6, 4	0	1, 3, 5, 7, 9, 11	15
BHSig-260	160	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	30
CEDAR	20	16, 14, 12, 10, 8, 6, 4	0	8, 10, 12, 14, 16, 18, 20	24

be because of the presence of diverse signature samples in the CEDAR.

To demonstrate the effectiveness of our proposed score-level fusion strategy compared to the feature-level fusion (concatenating LPQ and wavelet feature sets), and also signature verification using LPQ and wavelet feature sets alone, we evaluated all those models using all the datasets and the results are summarized in Figs. 5, 6, 7, and 8. From the results plotted on Figs. 5, 6, 7, and 8, it can be noted that in most of the cases, the wavelet features provide better results compared to the LPQ features. Furthermore, feature-level fusion demonstrates better signature verification performance (lower AERs) compared to the LPQ and wavelet features alone. However, the proposed score-level fusion method significantly increases (between 3 and 5%) the performance of our signature verification system compared to the systems using only the LPQ or wavelet-based features as well as the feature-level fusion strategy.

4.3 Comparative analysis

To compare our proposed method with other approaches, a number of state-of-the-art signature verification methods and a recent deep learning-based framework for signature verification are taken into account. A comparison of the

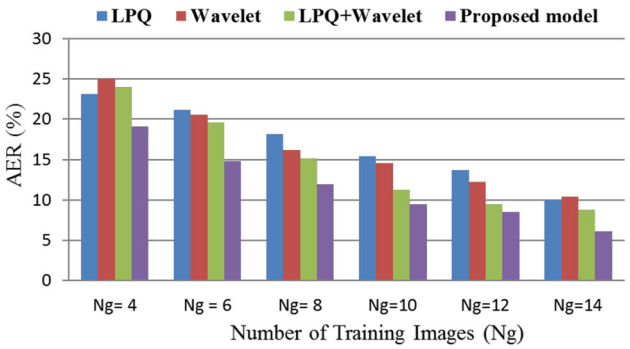

Fig. 5 AERs obtained from the proposed model, feature-level fusion, and LPQ and wavelet features separately on MCYT dataset

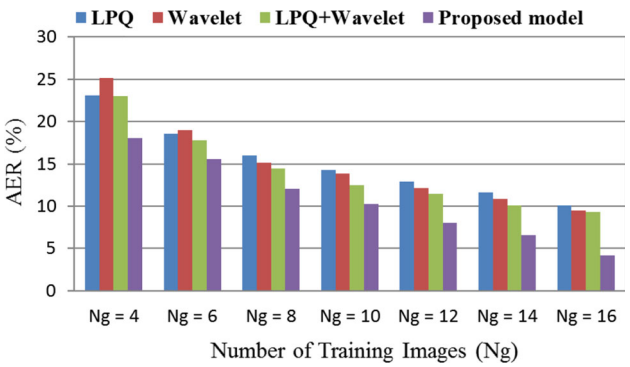

Fig. 6 AERs obtained from the proposed model, feature-level fusion, and LPQ and wavelet features separately on GPDS dataset

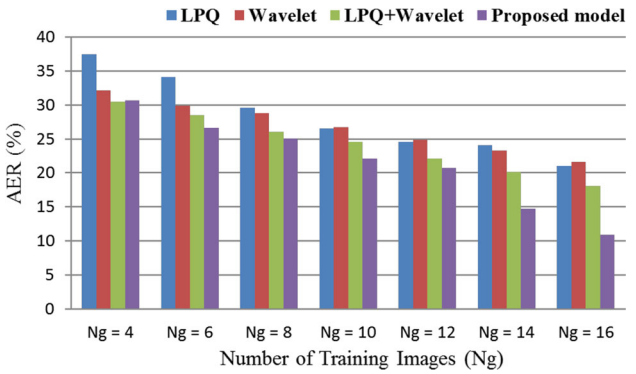

Fig. 7 AERs obtained from the proposed model, feature-level fusion, and LPQ and wavelet features separately on BHSig-260 dataset

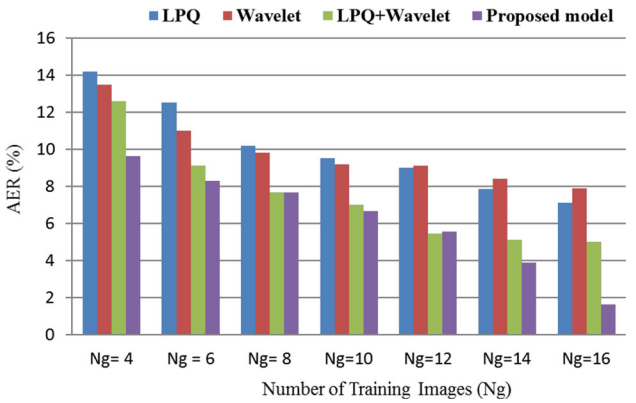

Fig. 8 AERs obtained from the proposed model, feature-level fusion, and LPQ and wavelet features separately on CEDAR dataset

results obtained from the proposed method using the optimal and general k for each dataset, and the results of other approaches presented in the literature on the MCYT, GPDS, CEDAR, and BHsig260 datasets are provided in Table 6. From the results shown in Table 6, it can be noted that the proposed method outperforms most of the state-of-the-art methods in terms of AER when 8, 12, or 16 signature samples were used for training the system. It is worth noting that as we used one-class SVMs in the proposed method and the one-class SVMs generally require enough data for training to achieve the best performance, the results obtained from the proposed system when a lesser number of signature images (e.g. 4) were used for training the proposed system are not that high as the results obtained from the system trained with 8, 12, and 16, but they are still comparable with the state-of-the-art methods.

To get an idea of the performance of deep learning and the use of a deep neural network (DNN) to learn the features instead of using the hand-crafted features, we considered a DNN, which a two-branch Siamese convolutional neural architecture, used in [40] to build a signature verification framework. The DNN [40] was trained using the same number of (4, 8, and 12) samples from the four

Table 6 Comparison of the AERs obtained from the proposed method with the other methods in the literature

Dataset	Method	No. of training samples	AER (%)
MCYT	Vargas et al. [10]	5	13.89
		10	10.07
	Alonso-Fernandez et al. [37]	10	22.48
	Proposed method (k = 2.18)	**4**	**19.11**
		10	9.50
		12	8.56
	Proposed method (k = 2.13)	4	19.16
		10	**9.26**
		12	**8.50**
GPDS-300	Eskander et al. [30]	12	15.24
		14	13.96
	Guerbai et al. [38]	4	16.92
		8	15.95
		12	15.07
	Ferrer et al. [45]	**4**	**16.10**
		8	14.15
		12	13.35
	Alaei et al. [35]	4	21.22
		8	13.80
		12	11.74
	Proposed method (k = 2.18)	4	18.01
		8	**12.06**
		12	**8.03**
BHsig260	Alaei et al. [35]	**4**	**28.88**
		8	**23.74**
		12	23.15
	Proposed method (k = 2.18)	4	30.66
		8	25.05
		12	20.76
	Proposed method (k = 2.11)	4	29.13
		8	24.80
		12	**20.11**
CEDAR	Kumar et al. [57]	16	6.02
	Chen et al. [58]	16	5.10
	Guerbai et al. [38]	**4**	**8.70**
		6	7.83
		12	5.60
	Proposed method (k = 2.18)	4	9.62
		6	7.66
		12	5.57
	Proposed method (k = 2.2)	4	9.50
		8	**7.59**
		12	**5.50**
		16	**1.64**

The bold values indicate the minimum AER values obtained from different systems using several number of samples for training from different datasets

datasets considered for training/testing the proposed model in this research work. The results obtained from the DNNs-based signature verification model (e.g. for CEDAR dataset, an AER of 5.13 was achieved when 12 samples from each individual were used for training and the rest were used for test) were very close to the results obtained from the proposed model in this paper. It is worth noting that DNNs suffer from under-fitting due to less training samples, and they generally require a large volume of data, here genuine and forgery signature images, for training to allow systems to be converged and provide promising results. However, in real signature verification scenarios, such as bank applications, it is difficult to collect a large number of forgery and genuine signatures from different individuals. Thus, we did not directly compare the results of the DNN baseline signature verification system with the results obtained from our proposed method.

5 Conclusion

In this research work, a classifier fusion strategy for signature verification based on two types of texture features, LPQ and wavelet, and one-class SVMs were proposed to combine two scores obtained from two types of information in order to achieve a higher signature verification performance. The proposed method provided considerably better results compared to the state-of-the-art methods using different offline handwritten signature datasets for experiments. From the results, it can be noted that the score-level fusion strategy is a better choice compared to the feature-level fusion. Furthermore, in real scenarios, when only genuine signatures are available for training/learning classifiers, one-class SVMs are suitable classifiers to be used for the classification/verification. Choosing a different type of features, which characterize different aspects of signature images, can also enhance signature verification performance.

Since in real world handwritten signatures can be written in different scripts, in future research, we plan to investigate the impact of merging different datasets with signatures written in different scripts/shapes on the signature verification performance.

References

1. Impedovo D, Pirlo G (2008) Automatic signature verification: the state of the art. IEEE Trans Syst Man Cybern Part C Appl Rev 38(5):609–635
2. Impedovo D, Pirlo G, Russo M (2014) Recent advances in offline signature identification. In: Proceedings of the 14th international conference on frontiers in handwriting recognition, pp 639–642

3. Hafemann LG, Sabourin R, Oliveira LS (2017) Offline handwritten signature verification—literature review. In: Proceedings of the 7th international conference on image processing theory, tools and applications (IPTA), pp 1–8
4. Leclerc F, Plamondon R (1994) Automatic signature verification: the state of the art-1989-1993. Intl J Pattern Recogn Artif Intell 8(3):643–660
5. Plamondon R, Srihari SN (2000) Online and off-line handwriting recognition: a comprehensive survey. IEEE Trans Pattern Anal Mach Intell 22(1):63–84
6. Malik MI, Ahmed S, Marcelliy A, Pal U, Blumenstein M, Alewijnse L, Liwicki M (2015) ICDAR 2015 competitions on signature verification and writer identification for on- and off-line skilled forgeries (SigWiComp 2015). In: Proceedings of the ICDAR, pp 1186–1190
7. Pottier I, Burel G (1994) Identification and authentication of handwritten signatures with a connectionist approach. In: Proceedings of the IEEE conference on neural networks, pp 2948–2951
8. Nguyen V, Kawazoe Y, Wakabayashi T, Pal U, Blumenstein M (2010) Performance analysis of the gradient feature and the modified direction feature for off-line signature verification. In: International conference on frontiers in handwriting recognition, pp 303–307
9. Yılmaz MB, Yanıkoğlu B (2016) Score level fusion of classifiers in off-line signature verification. Inf Fusion 32:109–119
10. Vargas JF, Ferrer MA, Travieso CM, Alonso JB (2011) Off-line signature verification based on grey level information using texture features. Pattern Recogn 44(2):375–385
11. Wang Z, Ying Z (2012) Facial expression recognition based on local phase quantization and sparse representation. In: Proceedings of the eighth international conference on natural computation (ICNC), pp 222–225
12. Kalera M, Srihari S, Xu A (2004) Offline signature verification and identification using distance statistics. Int J Pattern Recognit Artif Intell 18(7):1339–1360
13. Malik MI, Liwicki M, Dengel A (2011) Evaluation of local and global features for offline signature verification. In: Proceedings of the international workshop on automated forensic handwriting analysis, pp 26–30
14. Kumar R, Sharma JD, Chanda B (2012) Writer-independent off-line signature verification using surroundedness feature. Pattern Recogn Lett 33:301–308
15. Ruiz-Del-Solar J, Devia C, Loncomilla P, Concha F (2008) Offline signature verification using local interest points and descriptors. In: Proceedings of the 13th Iberoamerican congress on pattern recognition: progress in pattern recognition, image analysis and applications, pp 22–29
16. Malik MI, 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: Proceedings of the ICDAR, pp 1477–1483
17. Xu B, Lin D, Wang L, Chao H, Li W, Liao Q (2014) Performance comparison of local directional pattern to local binary pattern in off-line signature verification system. In: International congress on image and signal processing, pp 308–312
18. Pal S, Pal U, Blumenstein M (2013) A two-stage approach for English and Hindi off-line signature verification. In: Proceedings of the international workshop on emerging aspects in handwritten signature processing, pp 140–148
19. Pal S, Alaei A, Pal U, Blumenstein M (2011) Off-line signature verification based on background and foreground information. In: Proceedings of the international conference on digital image computing: techniques and applications, pp 672–677
20. Pal S, Alaei A, Pal U, Blumenstein M (2012) multi-script off-line signature identification. In: Proceedings of the international conference on hybrid intelligent systems, pp 236–240
21. Pal S, Nguyen V, Blumenstein M, Pal U (2012) Off-line Bangla signature verification. In: Proceedings of the international workshop on document analysis systems, pp 282–286
22. Pal S, Alaei A, Pal U, Blumenstein M (2015) Interval-valued symbolic representation based method for off-line signature verification. In: Proceedings of the IJCNN
23. Hu J, Chen Y (2013) Offline signature verification using real Adaboost classifier combination of pseudo-dynamic features. In: Proceedings of the 12th ICDAR, pp 1345–1349
24. Shanker AP, Rajagopalan AN (2007) Off-line signature verification using DTW. Pattern Recogn Lett 28:1407–1414
25. Justino EJR, El Yacoubi A, Bortolozzi F, Sabourin R (2000) An off-line signature verification system using HMM and graphometric features. In: Proceedings of the Fourth DAS, pp 211–222
26. Ferrer MA, Vargas F, Travieso CM, Alonso JB (2010) Signature verification using local directional pattern (LDP). In: Proceedings of the IEEE international Carnahan conference on security technology (ICCST), pp 336–340
27. Wen J, Fang B, Tang Y, Zhang T (2009) Model-based signature verification with rotation invariant features. Pattern Recogn 42(7):1458–1466
28. Gilperez A, Alonso-Fernandez F, Pecharroman S, Fierrez J, Ortega-Garcia J (2008) Off-line signature verification using contour features. In: Proceedings of the ICFHR
29. Fierrez-Aguilar J, Alonso-Hermira N, Moreno-Marquez G, Ortega-Garcia J (2004) An off-line signature verification system based on fusion of local and global information. Workshop on biometric authentication. Springer LNCS-3087. Springer, Berlin, pp 298–306
30. Eskander G, Sabourin R, Granger E (2013) Hybrid writer-independent-writer-dependent offline signature verification system. IET Biom 2(4):169–181
31. Batista L, Granger E, Sabourin R (2012) Dynamic selection of generative–discriminative ensembles for off-line signature verification. Pattern Recogn 45(4):1326–1340
32. Shekar BH, Bharathi RK, Kittler J, Vizilter Y, Mestestskiy L (2015) Grid structured morphological pattern spectrum for off-line signature verification. In: Proceedings of the international conference on biometrics (ICB), pp 430–435
33. Hamadene A, Chibani Y (2016) One-class writer-independent offline signature verification using feature dissimilarity thresholding. IEEE Trans Inf Forensics Secur 11(6):1226–1238
34. Ferrer MA, Vargas JF, Morales A, Ordonez A (2012) Robustness of offline signature verification based on gray level features. IEEE Trans Inf Forensics Secur 7(3):966–977
35. Alaei A, Pal S, Pal U, Blumenstein M (2017) An efficient signature verification method based on an interval symbolic representation and a fuzzy similarity measure. IEEE Trans Inf Forensics Secur 12(10):2360–2372
36. Guler I, Meghdadi M (2008) A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm. Digit Signal Proc 18(6):940–950
37. Alonso-Fernandez F, Fairhurst MC, Fierrez J, Ortega-Garcia J (2007) Automatic measures for predicting performance in off-line signature. Proc IEEE Intl Conf Image Process 1:369–372
38. 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 Recogn 48(1):103–113
39. Vargas JF, Travieso CM, Alonso JB, Ferrer MA (2010) Off-line signature verification based on gray level information using wavelet transform and texture features. In: Proceedings of the ICDAR, pp 587–92

40. Dey S, Dutta A, Toledo JI, Ghosh SK, Lladós J, Pal U (2017) SigNet: Convolutional Siamese network for writer independent offline signature verification. arXiv preprint arXiv:1707.02131
41. Simon C, Levrat E, Bremont J, Sabourin R (1997) A fuzzy perception for off-line handwritten signature verification. In: BSDIA'97, pp 261–272
42. Madasu VK, Yusof MHM, Hanmandlu M, Kubik K (2003) Off-line signature verification and forgery detection system based on fuzzy modeling. In: Gedeon TD, Fung LCC (eds) Advances in artificial intelligence, vol 2903. Springer, Berlin, pp 1003–1013
43. Hanmandlu M, Yusof MHM, Madasu VK (2005) Off-line signature verification and forgery detection using fuzzy modeling. Pattern Recogn 38(3):341–356
44. Woo YW, Han S, Jang KS (2006) Off-line signature verification based on directional gradient spectrum and a fuzzy classifier. In: Proceedings of the first pacific rim symposium (PSIVT 2006), pp 1018–1029
45. Ferrer M, Alonso J, Travieso C (2005) Offline geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Trans Pattern Anal Mach Intell 27(6):993–997
46. Prakash HN, Guru DS (2010) Offline signature verification: an approach based on score level fusion. Int J Comput Appl 1:52–58
47. Otsu N (1979) A threshold selection method from gray-level histograms. IEEE Trans Syst Man Cybern 9(1):62–66
48. Ojansivu V, Heikkilä J (2008) Blur insensitive texture classification using local phase quantization. Springer LNCS 5099:236–243
49. Mallat SG (1989) A theory for multiresolution signal decomposition: the wavelet representation. IEEE Trans Pattern Anal Mach Intell 11(7):674–693
50. Schölkopf B, Platt J, Shawe-Taylor J, Smola A, Williamson R (2001) Estimating the support of a high dimensional distribution. Neural Comput 13(7):1443–1472
51. Xu L, Krzyzak A, Suen CY (1992) Methods of combining multiple classifiers and their applications to handwriting recognition. IEEE Trans Syst Man Cybern 22:418–435
52. Kuncheva LI (2004) Combining pattern classifiers: methods and algorithms. Wiley Inter-science, London
53. Gader PD, Mohamed MA, Keller JM (1996) Fusion of handwritten word classifiers. Pattern Recogn Lett 17:577–584
54. Ortega-Garcia J, Fierrez-Aguilar J, Simon D, Gonzalez J (2003) MCYT baseline corpus: a bimodal biometric database. IEE Proc Vis Image Signal Process 150(60):395–401
55. Vargas F, Ferrer MA, Travieso CM, Alonso JB (2007) Off-line handwritten signature GPDS-960 corpus. In: Proceedings of the 9th ICDAR, pp 764–768
56. Pal S, Alaei A, Pal U, Blumenstein M (2016) Performance of an off-line signature verification method based on texture features on a large indic-script signature dataset. In: Proceedings of the DAS, pp 272–277
57. Kumar MM, Puhan NB (2014) Off-line signature verification: upper and lower envelope shape analysis using chord moments. IET Biom 3:347–354
58. Chen S, Srihari S (2006) A new off-line signature verification method based on Graph. In: Proceedings of the 18th international conference on pattern recognition, pp 869–872