DCT-SVM-Based Technique for Off-line Signature Verification

B. H. Shekar and R. K. Bharathi

Abstract In this paper, a new method for off-line signature verification is proposed based on discrete cosine transform (DCT). The proposed approach has two stages, namely feature extraction and representation of signature using DCT followed by classification through support vector machine (SVM). The training signature samples are subjected to preprocessing to obtain binarized image, and DCT is employed on the binarized image. The upper-left corner block of size $m \times n$ is chosen as a representative feature vector for each trained signature sample. These small feature vector blocks are fed as an input to the SVM for training purpose. The SVM is used as a verification tool and trained with different number of training samples including genuine, skilled, and random forgeries. The proposed approach produces excellent results on the standard signature databases, namely CEDAR, GPDS-160, and MUKOS—a Kannada signature database. In order to demonstrate the superiority of the proposed approach, comparative analysis is provided with many of the standard approaches.

Keywords Discrete cosine transform · Support vector machine · Signature verification

B. H. Shekar (✉)
Department of Computer Science, Mangalore University, Mangalore, Karnataka, India
e-mail: bhshekar@gmail.com

R. K. Bharathi
Department of Master of Computer Applications, S.J. College of Engineering, Mysore, Karnataka 570001, India
e-mail: rkbharathi@hotmail.com

1 Introduction

Biometric recognition in general forms a strong link between a person and his/her identity as the biometric traits cannot be easily shared, lost, or duplicated. Handwritten signature in particular happens to be the most natural behavioral biometric which generally established mode of providing the personal identity for authentication. The signatures have been established as one of the most acceptable means for authenticating a person's identity by many of the administrative and financial institutions [9]. Though human signature is a behavioral, natural, and intuitive, there exist few limitations in using this as the mode for personal identification and verification, such as there are some inconsistencies to a person's signature due to physical health, due to course of age, psychological or mental status, and so on [4]. The major threat/challenge in signature verification is the forgery of the signature, an illegal modification or reproduction of a signature. A signature is also considered forged if it is claimed that it was made by someone who did not make it [18]. Here, forgeries can be classified into three basic types: random forgery, when the forger has the access neither to the genuine signature nor to any information about the author's name, still reproduces a random signature; simple forgery, where the forger has no access to the sample signature but knows the name of the signer; and lastly, skilled forgery, when forger reproduces the signature, having access to the sample genuine signature. The signature is classified as online signature and off-line signature based on the procedure of capturing them. Online signature acquired at the time of its registration provides the intrinsic dynamic details, viz. velocity, acceleration, direction of pen movement, pressure applied and forces, whereas in off-line signature, the static image of the signature is captured once the signing process is complete. In spite of the fact that off-line signature lacks the dynamic details, it withholds many of the global and local features, viz. signature image area, height, width, zonal information, characteristic points such as end points, cross points, cusps, loops, presence and absence of zonal information. Devising an efficient and accurate off-line signature verification algorithm is a challenging task, as signatures are sensitive to geometric transformations, interpersonal signature in a corpus, complex background, skilled forgery, scalability of the system, noise introduced while capturing the image, difference in pen width, ink pattern, and so on. In this context, we proposed an efficient and simple to implement DCT-SVM technique for verification of the off-line signatures. The details of the proposed technique are brought out in the following subsections. The paper is organized as follows. Review of the related works is brought down in Sect. 2. In Sect. 3, we present the proposed technique. In Sect. 4, the experimental setup and a brief note on the dataset used in the experimentation along with the result analysis are presented. Comparative analysis of the proposed work with the work in literature is brought down in Sect. 5, followed by conclusion in Sect. 6.

2 Review of Related Work

Features play a vital role in the pattern recognition problems; hence, feature selection and extraction contribute significantly in the overall performance of any recognition algorithms. Off-line signatures are the scanned images of the signatures and possess three types of features, namely global, statistical, and geometrical features. The global features describe the signature image as a whole, statistical feature is extracted from the distribution of pixels of a signature image. The geometrical and topological features describe the characteristic geometry and topology of a signature, thereby preserving both global and local properties [1].

Some of the well-accepted off-line signature verification methods based on varying features and feature selection/extraction techniques have been introduced by many researchers. Huang and Yan [8] proposed a combination of static and pseudo-dynamic structural features for off-line signature verification. Shekar and Bharathi [19] concentrated on reducing the dimension of feature vectors, preserving the discriminative features obtained through principal component analysis on shape-based signature, and extended model is given based on kernel PCA [20]. Rekik et al. [16] has worked on the features consisting of different kinds of geometrical, statistical, and structural features. For comparison, they have used two baseline systems, global and local, both based on a larger number of features encoding the orientations of the stroke using mathematical morphology, and experimented on BioSecure DS2 and GPDS off-line signature databases. Kumar et al. [13] proposes a novel set of features based on surroundedness property of a signature image. The surroundedness property describes the shape of a signature in terms of spatial distribution of black pixels around a candidate pixel, which provides the measure of texture through the correlation among signature pixels in the neighborhood of that candidate pixel. They also developed the feature reduction techniques and experimented on GPDS-300 and CEDAR datasets. Kalera et al. [10] extracts the features based on quasi-multi-resolution technique using gradient, structural, and concavity (GSC) which was earlier used for identifying the individuality of handwriting, and experimented on CEDAR dataset. Nguyen and Bluemnstein [14, 15] concentrate on the global features derived from the total energy a writer uses to create their signature following the projections (both horizontal and vertical), which focuses on the proportion of the distance between the key strokes. They also described a grid-based feature extraction technique that utilizes directional information extracted from the signature contour and applied 2D Gaussian filter on the feature matrices. Chen and Srihari [2] tries to look at the online flavor in off-line signature by extracting the contours of the signature and combining the upper and lower contours neglecting the smaller middle portion to define a pseudo-writing path. To match two signatures, dynamic time warping (DTW), a nonlinear normalization is applied to segment them into curves, followed by extraction of features using Zernike moments (shape descriptor) and experimental results were given for CEDAR dataset. Ruiz-Del-Solar et al. [17] claims a new approach of using local interest

points in the signature image followed by computing local descriptors in the neighborhood of these points and later compared using local and global matching procedures. Verification is achieved through Bayes classifiers on GPDS signature corpus. Vargas et al. [21] focuses on pseudo-dynamic characteristics, that is, features presenting information of high-pressure points (HPP) of a handwritten signature contained in a grayscale image are analyzed. They used KNN and PNN standard model to analyze the robustness of simple forgeries of their own GPDS-160 signature corpus. Kumar et al. [12] comes with the objective in two-fold: one to propose a feature set based on signature morphology and the second is to use a feature analysis technique to get a more compact set of features that in turn makes the verification system faster through SVC on CEDAR signature database. Vargas et al. [22] work at the global image level and measure the gray-level variation in the image using statistical texture features, and the co-occurrence matrix and local binary pattern are analyzed and used as features. Experimental analysis is given using both random and skilled forgery for training and testing considering SVM classifier on MCYT and GPDS datasets. Ferrar et al. [5] present a set of geometric features based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates and tested with different classifiers such as HMM, SVM, and Euclidean distance classifier on GPDS-160 dataset. Thus, we have seen different class of algorithm that aims to achieve better classification accuracy. In this context, we devised a transform-based approach that exhibit compact representation and SVM is used for accurate classification. The details of the proposed technique are brought out below.

3 Proposed Model

The proposed DCT-SVM technique of off-line signature verification involves three major phases: preprocessing, DCT-based feature extraction, and SVM-based verification. In the preprocessing stage, the signature images are binarized using Otsu's method to remove the complex background which might have occurred due to scanning, ink distribution, and so on. Once we binarize the signature image, the noise is eliminated using a simple morphological filter that results in a clear noise-free signature image. This preprocessed image is transformed to frequency domain using discrete cosine transform (DCT) (see Fig. 1).
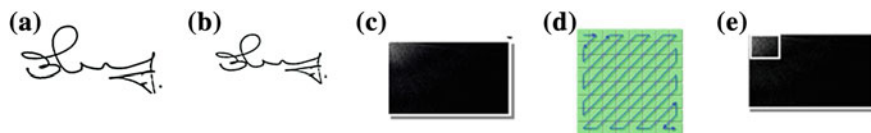
Fig. 1 a Initial image. **b** Binarized and noise removed. **c** DCT-transformed image. **d** Block feature of DCT coefficients and their selection in zigzag pattern. **e** Marked *top-left* block of the image (feature block)

Discrete Cosine Transform: The DCT is a popular technique in image processing and video compression which transforms the input signal present in the spatial domain into a frequency domain. We proposed to use DCT-II in our work introduced by Wang [23]. The forward 2D DCT of M X N block image **f** is defined as

$$C(u,v) = \propto (u).\propto (v) \sum_{X=0}^{M-1} \sum_{Y=0}^{N-1} f(x,y) X \cos\left[\frac{\pi(2x+1)u}{2M}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (1)$$

and the inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v) X \cos\left[\frac{\pi(2x+1)u}{2M}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (2)$$

where

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{M}}, & u = 0 \\ \sqrt{\frac{2}{M}}, & u = 1,2,\ldots M-1 \end{cases} \quad (3)$$

and x and y are spatial coordinates in the image block, and u and v are coordinates in the transformed image. It is well-known fact that the discriminative features are available in the top-left portion of the image, say of size $M \_N$, that is, the most energy being compacted to the low-frequency coefficients. The size of the subset is chosen such that it can sufficiently represent the input signature image and help in verification later. The size of the subset may be quite small compared to the whole vector with all the coefficients in it. It was observed that the DCT coefficients exhibit the expected behavior in which a relative large amount of information about the original signature image is stored/represented in fairly small number of coefficients [6]. The DCT coefficients, which are located at the upper-left corner, hold most of the image energy and have considered for further processing. For instance, the top $10 \times 10 = 100$ DCT coefficients are enough to represent the signature image and hence considered as a feature vector in our approach [11].

4 Experimental Setup and Result Analysis

The performance is evaluated through false acceptance rate (FAR) and false rejection rate (FRR). The FAR is the frequency that an unauthorized person signature (forge) is accepted as authorized (genuine), whereas the FRR is defined as the frequency that an authorized person (genuine) is rejected their access considering their signature to be forged. Hence, FAR is the percentage ratio of the total number of accepted forgeries to the total number of tested forgeries, whereas FRR is defined by the percentage ratio of total number of genuine rejected to the total number of tested genuine.

For the purpose of classification, we proposed to use support vector machine (SVM) classifier [7]. Unlike other techniques, where radial basis function (RBF) kernel [5] is used for training the system, we proposed to use linear kernel to reduce computational complexity. It is understood from the literature that the linear kernel performs well in terms of classification accuracy also. Training the SVM with suitable number of genuine and forgery (considered to be two-class problem) is a challenging task. We have conducted an exhaustive experimentation to exhibit the performance of the proposed algorithm with varying number of training and testing signature combinations. The training and testing samples include genuine signatures with random forgery and skilled forgery. Experimentation was conducted by extracting varying number of DCT coefficients from the DCT-transformed image, starting from dimension 8, that is, 64 coefficients, then to 10 with 100 coefficients and moved up to 14. Out of the experimental results analyzed, we decided to have 10×10 DCT coefficients as the feature vector for our rest of the experimentations. Extensive experimentation is conducted on publicly available databases, namely GPDS-160, CEDAR including one regional language database called MUKOS (Mangalore University Kannada Off-line Signature). Various combinations of samples are considered for training through SVM and hence testing to exhibit the efficacy of the proposed algorithm.

Initially, we started training the SVM with first 5 genuine and first 5 skilled forge samples from each signer of the dataset and tested with the remaining samples of genuine and skilled forge of corresponding signer. Later, we extended to train with first 10 genuine and first 10 skilled forge of each signer in the dataset and test with remaining samples. Similarly, we also extended to train with first 15 genuine and first 15 skilled forge samples and test with remaining samples of each signer of the dataset. The performance accuracy with different training sets on all databases considered is revealed in Table 1. Then, the experimentation was continued with training the SVM by 70 % of the genuine sample along with 100 randomly chosen forge (random forgery is the genuine sample of the other signer) from every database and tested with the remaining 30 % of genuine and other 50 randomly chosen forge. To justify the random selection, the above experimentations are repeated 5 times.

Table 2 gives the best performances of the DCT-SVM technique on all the databases considered and experimented with both random and skilled forgery. In the proposed technique, 0 % of false acceptance is observed when trained and tested with random forgery on CEDAR dataset. This was observed when we

Table 1 Performance accuracy (FAR and FRR) of the proposed DCT-SVM technique

No. of training samples	CEDAR		GPDS-160		MUKOS-Set-1	
	FAR	FRR	FAR	FRR	FAR	FRR
First 5 genuine + 5 skilled forgeries	8.32	10.64	11.77	13.56	11.44	13.43
First 10 genuine + 10 skilled forgeries	7.35	8.75	11.24	10.33	8.24	11.76
First 15 genuine + 15 skilled forgeries	6.44	7.28	11.64	7.63	4.18	10.49

Note Testing samples are the remaining signatures of the respective datasets

Table 2 Best performances of the DCT-SVM technique

Dataset	Experimentation with genuine and random forgery			Experimentation with genuine and skilled forgery		
	Accuracy	FRR	FAR	Accuracy	FRR	FAR
CEDAR	95.76	4.24	0.0	92.72	7.28	6.44
GPDS-160	96.29	3.70	0.046	92.47	7.63	11.64
MUKOS-Set-1	94.62	5.46	0.025	89.61	10.49	4.18
MUKOS-Set-2	95.59	4.41	0.063	91.75	8.22	6.54

trained the system with 12 genuine and 24 random forgeries of each signer, keeping the FRR to 4.24 % with an accuracy of 95.76 %. MUKOS-Set-1 has the accuracy of 89.61 %, with FAR of 4.18 %. Low FAR also projects the good performance of the model as it avoids the forge to be accepted as genuine.

4.1 Experimentation on MUKOS Database

We have also worked on one regional language off-line signature database called MUKOS. The MUKOS database consists of two sets: Set-1 consisting of 1,350 signatures and Set-2 with 760 signatures. In Set-1, we collected 30 genuine signatures and 15 skilled forgeries from 30 distinct signers. Each genuine signature was collected using black ink on A4 size white paper featuring 14 boxes on each paper. Once the genuine signatures were collected by all thirty signers, the forgeries were produced imitating a genuine signature from the static image of the genuine after a time gap where they were allowed to practice the forgery of other signers (other than genuine signers). In Set-2, we collected 20 genuine and 20 skilled forgery samples from $38(19 + 19)$ different individuals. Skilled forgery was obtained by arbitrarily selecting the people who in practice used English for their genuine signature. These signatures were acquired with a standard scanner with 75 dpi resolution in an 8-bit grayscale image. MUKOS performance is exhibited in Table 3, with convincing accuracy of 89.61 % for Set-1 and 91.75 % on Set-2.

Table 3 Experimental results for MUKOS dataset

Proposed by	Feature	Classifier	Accuracy	FAR	FRR
Shekar and Bharathi [19]	Shape-based eigen-signature	Euclidean distance measure	93.00	11.07	6.40
Proposed algorithm Set-1	DCT coefficients	SVM	89.61	10.49	4.18
Set-2		SVM	91.75	8.22	6.54

5 Comparative Analysis

Apart from the above experimentations, we have also conducted the experiments as proposed in the literature, which we have considered for result analysis. For instance, [14] in each test, 12 genuine signatures and 400 random forgeries were employed for training, and remaining 59 genuine signatures were chosen from the remaining 59 writers along with the remaining 12 genuine samples for testing from the GPDS-160 corpus. Kumar et al., [12] have selected 5 individuals randomly and kept them aside as test data and the remaining 50 individuals comprise the training data with a combination of 274 genuine–genuine pairs and 576 genuine-forged pairs of each individual from CEDAR corpus.

5.1 Experimentation on CEDAR Database

In Table 4, we present the results on CEDAR database. It shall be observed that the proposed DCT-SVM-based approach exhibit better performance when compared to other approaches. Although the classification accuracy is similar to that of [3], it should be noted that the number of feature used are only 100. High-performance rate is shown by the proposed technique when tested on CEDAR dataset (both with skilled and random forge samples). To boost the performance, 0 % false acceptance has been recorded when trained and tested with random forgery, indicating 100 % rejection of forge samples.

5.2 Experimentation on GPDS-160 Database

GPDS-160, a subcorpus of GPDS-300, is used for experimentation for the analysis of the performance of DCT-SVM technique. Extensive experimentation was conducted with this dataset as the literature has revealed a variety of combinations of number of training and testing samples. However, the proposed DCT-SVM technique out performed considerably high with the accuracy of 92.47 % when

Table 4 Experimental results obtained for CEDAR dataset

Model proposed by	Feature type	No. of features	Classifier	Accuracy	FAR	FRR
Kalera et al. [10]	Word shape (GSC)	1,024	PDF	78.50	19.50	22.45
Chen and Srihari [2]	Zernike moments	640	DTW	83.60	16.30	16.60
Kumar et al. [12]	Signature morphology	44	SVM	88.41	1,159	11.59
Chen and Srihari [3]	Graph matching	>1,024 + 8	DTW	92.10	8.20	7.70
Kumar et al. [13]	Surroundedness	24 out of 44	SVM	91.67	8.23	8.33
Proposed algorithm	DCT coefficients	100	SVM	92.72	7.28	6.44

Table 5 Experimental results obtained for GPDS-300 corpus

Model proposed by	Feature type	No. of features	Classifier type	Accuracy	FAR	FRR
Ferrar et al. [5]	Geometric features	42 * 2 + 22 * 2 sequence	SVM	86.65	13.12	15.41
			HMM		12.60	14.10
Vargas et al. [21]	High-pressure points (HPP)	Two vectors * no. of HPP	KNN & PNN	87.67	14.66	10.01
Vargas et at. [22]	GLCM + LBP	>(4 + 4 * radius)	SVM	87.28	6.17	22.49
Solar et al. [17]	Local interest points + local descriptors	12 * no. of descriptors	Bayesian	84.70	14.20	16.40
Kumar et al. [13]	Surroundedness	29 selected	SVM	86.21	13.76	13.76
Nguven and Blumenstein [15]	MDF, energy, maxima and ratio	Every black pixel	SVM	82.25	17.25	17.25
Nguven & Blumenstein [14]	Grid based + 2D Gaussian filter	(12 * 6 * 4) * no. of grids formed	SVM	86.32	13.68	14.18
Proposed model	DCT coefficients	100	SVM	92.47	7.63	11.64

first 15 genuine sample and 15 skilled forgeries of every signer is used to train the SVM, and remaining 9 genuine and 15 skilled forgery samples of every signer is used for testing. The detail result analysis is shown in Table 5.

6 Conclusion

We have proposed an efficient, robust, and less computational cost technique for off-line signature verification. The prominent DCT features of a preprocessed signature are fed to the layers of SVM for training and hence recognized the genuine and forged signatures by testing the samples. Exhaustive experimentations were conducted to exhibit the performance of the proposed technique with varying training and testing configurations. We also demonstrated the performance on various datasets with state-of-the-art models and databases. The success of the proposed technique performance is revealed through FAR and FRR.

References

1. Arya S, Inamdar VS (2010) A preliminary study on various off-line hand written signature verification approaches. Int J Comput Appl 1(9):55–60
2. Chen S, Srihari S (2005) Use of exterior contours and shape features in off-line signature verification. In: ICDAR, pp 1280–1284
3. Chen S, Srihari S (2006) A new off-line signature verification method based on graph matching. In International conference on pattern recognition (ICPR06), vol 2, pp 869–872
4. Fairhurst MC (1997) Signature verification revisited: Promoting practical exploitation of biometric technology. Electron Commun Eng J 9:273–280
5. Ferrer M, Alonso J, Travieso C (2005) Off-line geometric parameters for automatic signature verification using fixed-point arithmetic. IEEE Trans Pattern Anal Mach Intell 27(6):993–997
6. Hafed ZM, Levine MD (2001) Face recognition using the discrete cosine transform. Int J Comput Vis 43(3):167–188
7. Hsu C-W, Chang C-C, Lin C-J (2003) A practical guide to support vector classification
8. Huang K, Yan H (2002) Off-line signature verification using structural feature correspondence. Pattern Recogn 35:2467–2477
9. Impedovo D, Pirlo G (2008) Automatic signature verification: the state of the art. IEEE Trans Syst Man Cybern C (Appl Rev) 38(5):609–635
10. Kalera MK, Srihari S, Xu A (2003) Off-line signature verification and identification using distance statistics. Int J Pattern Recogn Artif Intell 228–232
11. Khayam S (2003) The discrete cosine transforms (DCT): theory and application. Michigan State University
12. Kumar R, Kundu L, Chanda B, Sharma JD (2010) A writer-independent offline signature verification system based on signature morphology. In: Proceedings of the first international conference on intelligent interactive technologies and multimedia, IITM'10, pp 261–265, New York, NY, USA. ACM
13. Kumar R, Sharma JD, Chanda B (2012) Writer-independent off-line signature verification using surroundedness feature. Pattern Recogn Lett 33(3):301–308

14. Nguyen V, Blumenstein M (2011) An application of the 2D Gaussian filters for enhancing feature extraction in offline signature verification. In ICDAR'11, pp 339–343
15. Nguyen V, Blumenstein M, Leedham G (2009) Global features for the offline signature verification problem. In: Proceedings of the 2009 10th international conference on document analysis and recognition, pp 1300–1304, Washington, DC, USA. IEEE Computer Society
16. Rekik Y, Houmani N, Yacoubi MAE, Garcia-Salicetti S, Dorizzi B (2011) A comparison of feature extraction approaches for offline signature verification. In IEEE international conference on multimedia computing and systems, pp 1–6
17. 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, CIARP'08. Springer, Berlin, pp 22–29
18. Saikia H, Sarma KC (2012) Approaches and issues in offline signature verification system. Int J Comput Appl 42(16):45–52
19. Shekar BH, Bharathi RK (2011) Eigen-signature: a robust and an efficient offline signature verification algorithm. In International conference on recent trends in information technology (ICRTIT), June 2011, pp 134–138
20. Shekar BH, Bharathi RK, Sharmilakumari M (2011) Kernel eigen-signature: an offline signature verification technique based on kernel principal component analysis. In (Emerging Applications of Computer Vision), EACV-2011 Bilateral Russian-Indian Scientific Workshop, Nov 2011
21. Vargas FJ, Ferrer MA, Travieso CM, Alonso JB (2008) Off-line signature verification based on high pressure polar distribution. In: Proceedings of the 11th international conference on frontiers in handwriting recognition, ICFHR 2008, Aug 2008, pp 373–378
22. Vargas J, Ferrer M, Travieso C, Alonso J (2011) Off-line signature verification based on grey level information using texture features. Pattern Recogn 44(2):375–385
23. Wang Z (1984) Fast algorithms for the discrete w transform and for the discrete Fourier transform. IEEE Trans Acoust Speech Signal Process 32(4):803–816