Off-Line Signature Confirmation based on Cluster Representations of Geometrical and Statistical Features through Vector Distance, Neural Network and Support Vector Machine Classifiers

Aravinda Chikmagalur Ventakaramu
Department of Computer Science and Engineering, N.M.A.M. Institute of Technology Nitte, India
Aravinda.cv@nitte.edu.in

Suresha Devaraj
Department of Information Science and Engineering
A.J. Institute of Technology, India
sureshasss@gmail.com

Prakash Hebbakavadi Nanjundaiah
Department of Computer Science and Engineering, Rajeev Institute of Technology, India
Prakash_hn@yahoo.com

Kyasambally Rajasekhar Udayakumar Reddy
Department of Information Science and Engineering, Dayananda Sagar College of Engineering, India
vp.dsce@dayanandasagar.edu

Abstract: *We exploited the geometrical and statistical properties of signature images for offline signature verification and identification in this paper, using signature clustering and classification based on extracted features. The Offline-SVR has been tested on the 2004 Ministerio de Ciencia Tecnología e Innovación (MCTYTDB) OffLineSignSubCorpus dataset, the MCYT-330 online signature dataset, and the MCE-200 dataset, which together are referred to as the MCE-605 dataset. Using a standard data set for experiments, the results of the Vector Distance (VD), Support Vector Machine (SVM) and Neural Network (NN) methods are significantly superior to those of other signature verification and recognition methods. Moreover, the VD method performed better than The SVM and NN methods. The purpose of the study is on clustering signature images using geometric and statistical features, as well as the utilization vector distance, neural networks, and support vector machines for signature image verification and identification. It was decided to use the algorithm for developing geometric and statistical features. The signature images are classified using generated features using k-means clustering, and Offline and Online- Support Vector Regression (SVR) is accomplished using VD, SVM, and NN training and classification with a different number of signatures each time, preceded by verification using recognition statistics. Because of the minimal number of features, the designed mechanism seems to be much faster. Experimenting on a standard dataset reveals that the results obtained from clustering signatures and categorization are effective and simple in comparison to other Offline signature confirmation systems. In this research work, we address the problem of representing handwritten signatures (online/offline) suitable for effective verification and recognition. We propose effective feature extraction for verification and recognition of signatures.*

Keywords: *Offline signature confirmation, k-means clustering, geometrical feature, statistical feature, vector distance, neural network, support vector machine.*

Received July 14, 2020; accepted October 10, 2021
https://doi.org/10.34028/iajit/19/4/11

1. Introduction

Offline Signature Confirmation (Off-SC) [1, 2, 3] isn't just an area of research in digital image processing and pattern identification [4] in addition it is generally utilized for individual identification in businesses like banking systems [5], admittance control, legally binding issues with security. Basically, there are two forms of signature confirmation techniques to be specific the On-Line Signature Confirmation (On-SC) method and the Off-SC method. In the On-SC signature, the picture is acquired and investigated in real-time as the individual sign it. To acquire the signature of individual real-time On-SC [6, 7, 8, 9, 10, 11, 12, 13, 14] mechanism multitouch-sensitivity monitor and an electronic tablet were used to capture dynamic details for confirmation. Then extract details regarding the signature and record the movement of the stylus sensor during the instance of signature is created, which involves area, velocity, and acceleration with pressure on the stylus pen. The Off-SC scheme uses an optical scanner to get handwriting figures written a on document, dealing wi2D picture structure of the signature. Now steady vibrant characteristics were absent since the non-recurring environment of discrepancy of signature, because of aging, infirmity, geographic position with perchance to some amount of the expressive state of the individual will highlight the difficulty, accordingly, the Off-SC mechanism is composite. The researchers in these systems use neural Network Training and Classification (NNTC) [15], hidden Markova model [16], Support Vector Machine Training and Classification (SVMTC) [17, 18], discrete cosine transform [19, 20, 21], symbolic representation based advance in confirming signature.

The distinctive techniques and diverse list of features checking query signature. In our current research emphasis is on testing robust feature sets set obtained using geometric and statistical features present in the signature image. The mechanism for developing geometric and statistical features is shown in Figures 4 and 5 respectively. The generated features for genuine and forgery dataset are clustered using k-means clustering into 4 clusters for genuine and forgery respectively. Later cluster centroids are used in vector distance calculation, SVMTC and NNTC. The confirmation/ recognition statics in vector distance calculation, SVMTC and NNTC are shown in Table 1. The outlined algorithm works considerably faster due to modest list of feature set. The continued division of this article is structured as: portion 2 talk about detailed literature study, portion 3 light up proposed design. The obtained results of experimentation i.e., centroids of clustering results for genuine and forgery signature set and the error metric insights calculated in False Acceptance Rate (FAR), False Recognition Rate (FRR), Average Error Rate (AER) and Overall, Error Rate (OER) are conferred in portion 4 to conclude the article is summarized in portion 5.

2. Literature

All around validated conventional authentication method is signature confirmation and is an important verification in the financial sector of an individual person and on his behalf. The most effective viewpoint in signature investigation is psychological effect of signer on signing mode, and still, signatures are widely recognized biometric for all official intends to check an individual person identity in financial/administrative segment. Bansal *et al*. [3] applied algorithm-based contour matching for tracking characteristics pattern in signatures. Later HMM is applied for classification. Gruber *et al*. [5] used longest common subsequences detection for measuring the similarity of signature in applying SVM for On-SC. Guru and Prakash [6] applied symbolic representation on On-SC, in their experimentation they used interval valued symbolic feature for global feature and exploited writer dependent threshold for minimizing error rate. Ashok Kumar and Dhandapani [11] designed neural network model for signature testing and verification for Off-SC for bank cheques. Liu *et al*. [14] applied sparse representation with DCT for On-SC through compact representation using a fixed number of coefficients. Sae-Bae and Memon [17] in automatic Off-SC applied 2-level contourlet transform with directional textural features for forming feature vector. The exploration in signature examination is principally divided into On-SC and Off-SC. Wilkinson *et al*. [22] have used Dynamic Time Wrapping DTW to detect the forgeries. Verification assumes that the properties of the curvature, total length, and slant angle are constant among different sample signatures of an individual. The different researchers in On-SC and Off-SC utilized assessed the feasibility of Recurring Neural Network with Siamese architecture for the task of online signature verification. They proposed both long short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) system with Siamese architecture and obtained Equal Error Rate (EER) 5.28 (for Bidirectional Long Short-Term Memory BLSTM) and 2.92 for Gated Recurrent Unit (BGRU) system for different training scenario

3. Proposed Architecture

Off-SC is basically a pattern recognition issue that takes as input a query signature. The query signature is then compared to a signature set of preexisting datasets of a certain individual to ensure that the individual is authentic. Off-intended SC's architecture is divided into two key sections. Feature extraction and clustering is the first stage, which focuses on extracting features from pre-existing genuine and counterfeit datasets. The retrieved characteristics from the real and forgery datasets were grouped into four clusters for the genuine dataset and four clusters for the forgery dataset, with the centroid of each cluster calculated. The second step is query signature confirmation, which focuses on testing in three main areas for query signature confirmation. Vector distance, neural network training and classification, and SVM training and classification are the aspects that have been tested for confirmation. Tables 1 and 2 show the results of the experimentation.

3.1. Feature Extraction and Clustering Phase

Figure 1 depicts the flow of the feature extraction and clustering phase. This stage begins with a knowledge dataset on genuine and forgery signatures that has been predefined. Algorithms were used to extract geometrical and statistical features from genuine and forgery signatures. Geometric and statistical-features the feature vectors were clustered using k-means to form four clusters for the genuine vector set and four clusters for the forgery vector set, and their cluster centroids were obtained. Table 1 lists the cluster centroids for group 0002 of the datasets 2004 MCYTDB Offline Sign Sub Corpus.

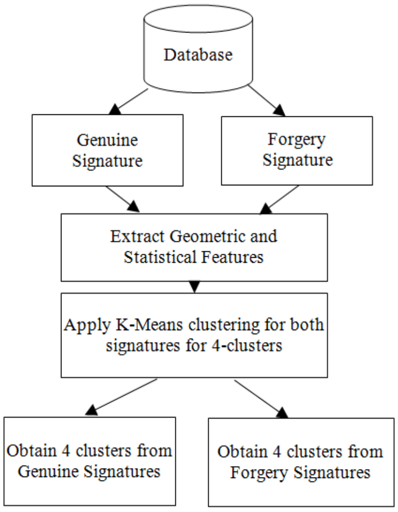

Figure 1. Feature extraction and clustering.

3.2. Confirmation of Query Signature Phase

The next stage is confirmation of query signature. The confirmation phase focus on confirmation of query signature i.e., to check whether query signature is genuine or forgery. The experimentation in confirmation stage is conducted in three main aspects, i.e., vector distance, neural network training and classification and SVM training and classification.

3.2.1. Confirmation based on Vector Distance

The experimentation in the confirmation step, as shown in Figure 2, begins with the input query signature. The geometry and statics of the query signature are retrieved using techniques 2 and 3 that are defined in vector space and tabulated. Through the minkowski distance between vectors, the recovered feature vector is compared to the centroids of genuine and forged signatures. Tables 1 and 2 show the outcomes of the experiments on the dataset 2004 MCYTDB OffLineSignSubCorpus.

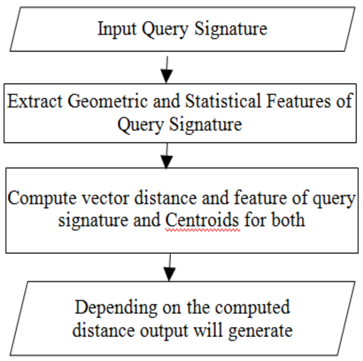

Figure 2. Query Signature confirmation based on vector distance.

3.2.2. Confirmation based on Neural Network Training and Classification

The second experimentation in confirmation stage conducted with neural network training and classification as shown in Figure 3.

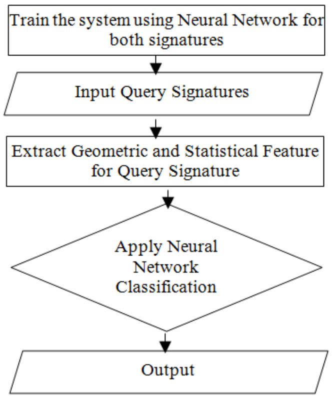

Figure 3. Query signature confirmation based on neural network training and classification.

Here before reading input query signature neural network is trained with cluster centroids of genuine and forgery vector set. Then the query signature is read and its geometric and statistics were extracted through the Algorithms (2) and (3) defined in and tabulated in vector space. The extracted feature vector is subjected to neural network classification with trained dataset and results of classification were announced. The results of experimentation on dataset 2004_MCYTDB_Offline Sign Sub Corpus are tabulated in Tables 1 and 2.

3.2.3. Confirmation based on SVM Training and Classification

Figure 4 depicts the next experimentation in the confirmation stage, which was carried out with SVM training and classification. Before reading the input query signature, SVM is trained with cluster centroids from the genuine and forgery vector sets. The query signature is then read, and its geometric and statistical information is extracted using the Algorithms (2) and (3) defined in and tabulated in vector space. The extracted feature vector was subjected to SVM classification with a trained dataset, and the classification results were published. Tables 1 and 2 show the results of experiments on the dataset 2004 MCYTDB Offline Sign Sub Corpus.

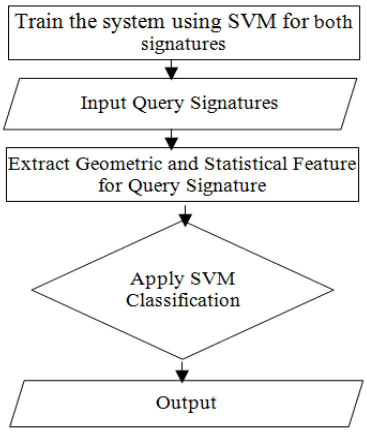

Figure 4. Query signature confirmation based on SVM training and classification.

4. Geometrical Feature Extraction (GeFE)

The four pixels were calculated in pixel point image depending on location of pixel points, i.e., minimum and maximum in X-direction named Xmin and Xmax and the minimum and maximum pixel points were found in Y-direction named Ymin and Ymax as shown in Figure 5.

Figure 5. Computation of Xmin, Xmax, Ymin and Ymax.

Algorithm 1: Geometric Feature
//Input: Signature image
//output: 32 geometric features consisting of 16 distance features & 16 angle features

begin
Step 1: Calculate the centroid(ct) for pixel points in signature image
Step 2: Divide pixel points in signature image into four partition centered at ct.
Step 3: Extract 4 pixels from each partition totaling 16 pixels using following criteria as per figure 5.
end

V: Statistical feature extraction (StFE)
The proposed algorithm for StFE works directly on input signature image and gives 10 statistical features of signature image. The proposed algorithm for StFE is shown in Algorithm below

Algorithm 2: Statistical Feature

//Input: Signature RGB color image
//output: 10 Statistical features.
begin
Step1: Preprocessing
Convert RGB signature to gray image
Step 2: Find top left and bottom right for fixing boundary for signature.
Step 3: Create the Gray Level Co-occurrence Matrices (GLCMs)for signature image
Step 4: Derive Statistics from GLCM& Signature image
end

5. Results and Discussion

The proposed algorithms shown in Figure 5 are experimented on 2004_MCYTDB_Offline SignSubCorpus dataset. Each group in dataset contains 15 genuine signatures and 15 forgery signatures. The experimentation on above dataset conducted in 2 stages, in the first stage the experimentation done with 4 genuine signature and 4 forgery signatures used for training in SVM and NN for each group and tested against all 30 signatures of that group.

The second phase is confirmation of query signature. The experimentation in confirmation phase is conducted in three main aspects:

- Vector distance.
- Neural network training and classification.
- SVM training and classification.

Once the cluster centroids for genuine and forgery signatures have been computed, all of the signatures in the group are tested against FAR, FRR, AER, and OER. FAR is used as a ratio of the number of false acceptances to the total number of detections attempts to determine the incorrect acceptance of a forgery signature. FRR is a measure of the incorrect rejection of a genuine signature; it is calculated as the ratio of the number of false rejections to the total number of detection attempts. The group's AER is the sum of its FAR and FRR. The OER is the average of all group error rates. The experimentation done on dataset with all 30 signatures in that group are sent for confirmation using above three aspects are tabulated in Table 2.

Table 1. SVM Training and classification for 2004_MCYTDB_offlinesignsubcorpus dataset.

Support Vector Machine (SVM)					
4 Authentic and 4 Forgery for training			8 Authentic and 8 Forgery for training		
FAR in %	FRR in %	AER in %	FAR in %	FRR in %	AER in %
28.8	5.334	17.067	25.334	4.002	14.668

The experimentation done on dataset with 4 Authentic and 4 Forgery signature in first stage and in next 8 Authentic and 8 Forgery signature used for training and all 30 signatures in that group are sent for verification using SVM classifier and tabulated in Table 1.

The experimentation repeated on dataset with 4 Authentic and 4 Forgery signature in first stage and in next 8 Authentic and 8 Forgery signature used for training and all 30 signatures in that group are sent for verification using NN classifier and tabulated in Table 2.

Table 2. N.N Training and classification for 2004_MCYTDB_OffLinesignsubcorpus dataset.

Neural Network (NN)					
4 Authentic and 4 Forgery for training			8 Authentic and 8 Forgery for training		
FAR in %	FRR in %	AER in %	FAR in %	FRR in %	AER in %
38.528	7.465	22.9965	24.534	14.856	19.695

6. Contribution of this Work

On the massive dataset, we ran tests to see how well the enhanced approaches performed. This dataset is divided into 75 folders, each of which comprises 25 samples, including 15 original samples and 10 fraud samples from various authors, as well as mixed data samples of 500 numbers. The following validation procedure was used in our trials. We used the folders of each writer's signature samples to train our classifiers. The identification performance is calculated using a test set made up of all untrained datasets. The accuracy of an approach's identification performance, which is the percentage of writers that it properly recognizes, is used to assess its performance. A higher identification analysis shows that an approach is more accurate. The performance of the classifier's identification is investigated for a series of list sizes, where the list size represents the number of writers the classifier can choose between. In all the tests, a 1-nearest neighbor classifier using chi-square distance is being used to classify the data. We utilized 1125 annoying writers in our statistical approach experiments. We deployed 750 distracting authors in the model-based approach. We merged features from the model-based approach with edge-hinge combinations. Combining features obtained by the edge hinge combination increases identification performance approximately 97%. As a result, a larger dataset is required to show that our combined technique is much better than Schumacher et al's. The results of the experiments is as shown in the figure form Figures 6, 7, 8, 9, and 10.

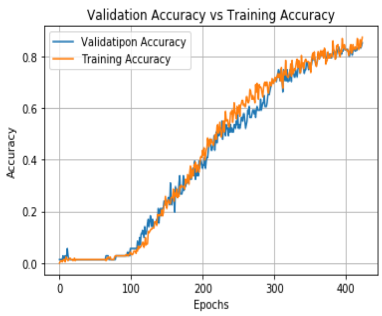

Figure 6. Validation accuracy v/s training accuracy.

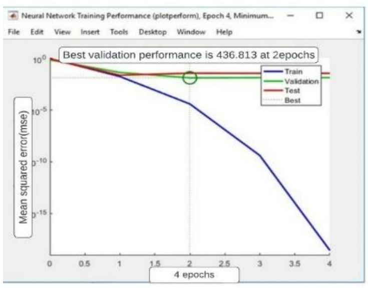

Figure 7. Best validation performance epoch 3.

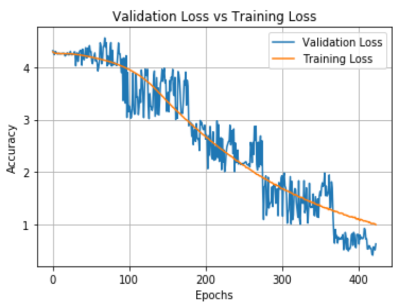

Figure 8. Validation loss v/s training Loss.

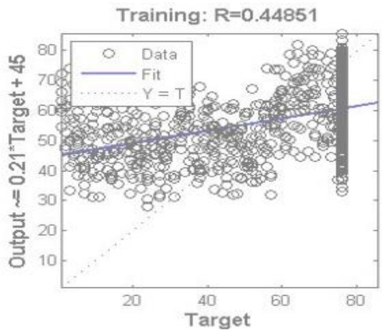

Figure 9. Training the target sample.

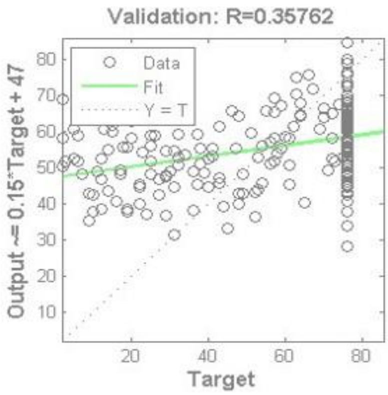

Figure 10. Target validation of the sample.

7. Conclusions

Individual signatures are an outstanding biometric distinguishing feature for identification of individuals in a wide variety of crucial areas, such as economics, admission control, contractual documentation, protection, and security. In this article, we applied k-means clustering, vector distance, and neural network training to extract geometrical and statistical features from the off-SC data. MCYTDB Offline Sign Sub Corpus data from 2004 was used to test the mechanisms. The analysis shows that OER has significantly less Vector Distance than other approaches, and the results are comparable to other approaches in the literature.

References

[1] Aravinda C., Meng L., and Reddy U., "An Approach for Signature Recognition Using Contours-Based Technique," *in Proceedings of International Conference on Advanced Mechatronic Systems*, Kusatsu, pp. 46-51, 2019.

[2] Aravinda C., Meng L., Reddy U., and Prabhu A., "Signature Recognition and Verification Using Multiple Classifiers Combination of Hu's and HOG Features," *in Proceedings of International Conference on Advanced Mechatronic Systems*, Kusatsu pp. 63-68. 2019.

[3] Bansal A., Garg D., and Gupta A., "A Pattern Matching Classifier for Offline Signature Verification," *in Proceedings of 1st International*

Conference on Emerging Trends in Engineering and Technology, Nagpur, pp. 1160-1163, 2008.

[4] Fayyaz M., Saffar M., Sabokrou M., Hoseini M., and Fathy M., "Online Signature Verification Based on Feature Representation," *in Proceedings of The International Symposium on Artificial Intelligence and Signal Processing*, Mashhad, pp. 211-216, 2015.

[5] Gruber C., Gruber T., Krinninger S., and Sick B., "Online Signature Verification with Support Vector Machines Based on LCSS Kernel Functions" *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 40, no. 4, pp. 1088-1100, 2010.

[6] Guru D. and Prakash H., "Online Signature Verification and Recognition: An Approach based on Symbolic Representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 6, pp. 1059- 1073, 2009

[7] Houtinezhad M. and Ghaffary H., "Improvement of Imperialist Competitive Algorithm based on the Cosine Similarity Criterion of Neighboring Objects," *The International Arab Journal of Information Technology*, vol. 18, no. 3, pp. 261-269, 2021.

[8] Iranmanesh V., Ahmad S., Adnan W., Yussof S., Arigbabu O., and Malallah F., "Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis," *The Scientific World*, pp. 357-360, 2011.

[9] Julita A., Fauziyah S., Azlina O., Mardiana B., Hazura H., and Zahariah A., "Online Signature Verification System," *in Proceedings of 5th International Colloquium on Signal Processing and its Applications*, Kuala Lumpur, pp. 8-12, 2009.

[10] Justino E., Bortolozzi F., and Sabourin R., "Off-Line Signature Verification Using HMM for Random, Simple and Skilled Forgeries," *in Proceedings of 6th International Conference on Document Analysis and Recognition*, Seattle, pp. 1031-1034, 2001.

[11] Kumar A. and Dhandapani S., "A Bank Cheque Signature Verification System using FFBP Neural Network Architecture and Feature Extraction based on GLCM," *International Journal of Emerging Trends\and Technology in Computer Science*, vol. 3, no. 3, pp. 46-52, 2014.

[12] Kanungo T., Mount D., Netanyahu N., Piatko C., Silverman R., and Wu A., "An Efficient K-Means Clustering Algorithm: Analysis and Implementation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 881-892, 2002.

[13] Li N., Liu J., Li Q., Luo X., and Duan J., "Online Signature Verification Based on Biometric Features," *in Proceedings of 49th Hawaii International Conference on System Sciences*, Koloa, pp. 5527-5534, 2016.

[14] Liu Y., Yang Z., and Yang L., "Online Signature Verification Based on DCT and Sparse Representation," *IEEE Transactions on Cybernetics*, vol. 45, no. 11, pp. 1-14, 2014.

[15] Padmajadevi G. and Aprameya K., "Comparison of Offline Signature Verification Systems with Support Vector Machines and Neural Network Classifiers Using Geometrical," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 6. no. 8, pp. 16181-16190, 2017.

[16] Pushpalatha K., Prajwal S., Gautam A., and Kumar K., "Offline Signature Verification Based on Contourlet Transform and Textural Features Using HMM," *in Proceedings of International Conference on Recent Advances and Innovations in Engineering*, Jaipur, pp. 1-6, 2014.

[17] Sae-Bae N. and Memon N., "Online Signature Verification on Mobile Devices," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 933-947, 2014.

[18] Sae-Bae N. and Memon N., "A Simple and Effective Method for Online Signature Verification," *in Proceedings of International Conference of the BIOSIG Special Interest Group*, Darmstadt, pp. 1-12, 2013.

[19] Sarfraz M. and Rizvi S., "An intelligent system for Online Signature Verification," *in Proceedings of 2nd International Conference on Information Security and Cyber Forensics*, Cape Town, pp. 1722, 2015.

[20] Tolosana R., Rodriguez R., et. al., "ICDAR 2021 Competition on On-Line Signature Verification," *in Proceedings of International Conference on Document Analysis and Recognition*, pp. 723-737, 2021.

[21] Venkataramu A., Masahiko A., Akshaya A., Gurupura A., and Rajashekar U., "Offline Signature Recognition and Verification Using ORBKey Point Matching Techniques," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 4, pp. 1-7, 2020.

[22] Wilkinson T., Pender D., and Goodman J., "Use of Synthetic Discriminant Functions for Hand-Written Signature Verification," *Applied Optics*, vol. 30, no. 23, pp. 3345-3353, 1991.

Aravinda Chikmagalur Ventakaramu is currently has an Associate Professor in the Department of Computer Science and Engineering at N.M.A.M Institute of Technology Nitte, Karkala. He received his bachelor's and master's degree in Computer Science from Mysore University and a Ph.D. degree from Visvesvaraya Technological University Belagavi. He has received his Research Fellowship from Ritsumeikan University Japan. He has authored several peer-reviewed national and international conferences Journal papers.

Suresha Devaraj currently working as Professor at Department of Information Science and Engineering at A.J Institute of Engineering and Technology, Mangaluru. He received his Bachelor of Engineering degree from Kuvempu University, Shankaraghatta, MTech and Ph.D. degree from Visveswaraya Technological University, Belagavi, Karnataka, India. He has published various Research Papers at reputed Journals/International Conference. He is reviewer of few Journals and International Conferences.

Prakash Hebbakavadi Nanjundaiah currently working has a Professor in the Department of Computer Science and Engineering at Rajeev Institute of Technology, Hassan, India. He received his B.E. degree in Electronics and Communication Engineering from the University of Mysore, Mysore, India, in 1990 and the MTech degree in Electronic Instrumentation from Regional Engineering College, Warangal, India in 1995 respectively. He received the Ph.D. degree in Computer Science and Engineering from the University of Mysore, Mysore, India, in 2010. He has authored several peer reviewed papers at national and international conferences and Journals Including IEEE Transactions. His research interest includes signature analysis and retrieval, clustering, biometrics, Image processing, Pattern recognition and symbolic data analysis. Dr. Prakash is a life member of Indian professional bodies such as Institute of Engineers, Indian Society for Technical Education (ISTE) and System Society of India (SSI) and Member of Indian Institute of Engineers, India.

Kyasambally Rajasekhar Udayakumar Reddy currently working has Vice-Principal and Professor, Dept of ISE at Dayanand Sagar College of Engineering and Management Bangalore. He served has Professor and Head in Computer Science and Engineering, NMAM Institute of Technology, Nitte, from May 2016 to July 2021. Professor of Computer Science and Engineering, NMAM Institute of Technology, Nitte, from August 2015 to April 2016.Professor in Computer Science and Engineering, BNM Institute of Technology, Bangalore, from August 2010 to July 2015.Assistant Professor in Information Science and Engineering, BNM Institute of Technology, Bangalore, from February 2004 to June 2007.