

## Offline Signature Verification with Random and Skilled Forgery Detection Using Polar Domain Features and Multi Stage Classification-Regression Model

K. N. Pushpalatha<sup>1</sup>, Aravind Kumar Gautham<sup>2</sup>, D. R. Shashikumar<sup>3</sup>,  
K. B. ShivaKumar<sup>4</sup> and Rupam Das<sup>5</sup>

<sup>1</sup>Research Scholar, Mewar University,  
Chittorgarh, Rajasthan, India.

<sup>2</sup>Principal, S D College of Engineering,  
Muzaffarnagar, U P, India.

<sup>3</sup>Professor, Department of ISE, Cambridge Institute of Technology,  
Bangalore, India.

<sup>4</sup>Professor, Department of TCE, Sri Siddhartha Institute of Technology,  
Tumkur, Karnataka

<sup>5</sup>Head, Research Division

Integrated Ideas, Gulbarga, Karnataka

<sup>1</sup>knpdrs@gmail.com, <sup>2</sup>drakgautamsd@gmail.com, <sup>3</sup>shashikumardr@yahoo.com,  
<sup>4</sup>kbssit@gmail.com, <sup>5</sup>rupam.iics@gmail.com

### Abstract

Offline signature verification system finds several applications in monitory transaction systems like banks. However one of the major challenges in this direction is the capability of the system to detect skilled and unskilled forgery. Many cases of bank check forgeries have been reported. Most of the offline signature verification system adopts recognition based technique where the system classifies a given signature sample as one of the samples from the database. However detection of a forgery in a given sample is challenging as the input sample looks similar to one of the samples in the database. In this paper we propose an innovative approach for offline signature verification with polar feature descriptor for signature that contains Radon Transform and Zernike Moments. Verification is performed using Multiclass Support Vector Machine. Once a signature is verified as being of a registered class, PLS Regression is applied on the sample against all samples in the database of the verified user to obtain regression score. Log Likelihood of the sample against all sample of the user is calculated using Hidden Markov Model. Authenticity of the classification is justified if the regression score and Log Likelihood distance deviation is less than 5%. Results show that the system verifies signature with an accuracy of 98% with false acceptance rate of .8%. Proposed system also detects skilled forgery with an accuracy of 71% and Random forgery with an accuracy of 76%.

**Keywords:** Offline Signature Verification, Skilled Forgery Detection, Hidden Markov Model, Partial Least Mean Square Regression, Support Vector Machine, Curvelet Transform, Radon Transform, Zernike Moments

## 1. Introduction

Signature verification is one of the primitive personal verification systems [1]. Signature verification system can be online or offline. In online signature verification system [2], user is asked to write his signature on a drawing panel. Relative position, Stroke, Pressure and direction of the stroke are measured and are used as feature descriptors. It is then classified using with any of the classifiers. HMM [3] and Neural Network [4, 5] are one of the two most popular classifier for online signature verification system. Users use either digital pen or fingers on touch pad to "draw" their signature. As number of feature descriptors is low, development of an efficient online signature verification is easy. Further every user tends to follow same direction for signing. Thus a forgery can be detected by analysing direction vector of the signature [6].

Online Signature Verification system finds its application in digital transactions and authentication system. However a wider use of signature verification system is found in offline signature verification system. Such systems are used in almost everywhere, in every document for attestation of the user.

There are several challenges in building an efficient offline signature verification system. Some of technically challenging aspects for building an offline Signature verification system are:

- ✓ *Direction vector cannot be obtained from offline signatures.*
- ✓ *Offline signature is digitized by scanning which introduces sampling and quantization noise*
- ✓ *Background of signature is not always white. Hence segmenting the signature is a challenge.*
- ✓ *Signature dimension varies from one instance to another.*
- ✓ *Inclination angle varies from one instance to another*
- ✓ *Determining stroke and pressure is difficult*

Therefore an offline signature verification system should meet above mentioned challenges for an efficient verification system.

Furthermore mere verification is not sufficient for an effective offline signature verification system. The system should be capable of identifying forgery. There are several types of forgery which includes Skilled Forgery, Novice Forgery, Random Forgery etc. Forgery is a case where an imposter tries to imitate the signature of a valid user and is very difficult to authenticate by linear model. Hence the system should use a probabilistic model to check the probability of signature being belonging to a person by validating it against all the signature samples of the same person.

## 2. Related Works

Several works are published in offline verification system. Works differ mainly in feature extraction and classification techniques. Signatures are mainly complex and cursive shapes. Therefore they are described best with shape features. However shapes are considered as global entity and therefore are not widely studied in offline signature verification system. Moments like Zernike Moments and Thin plate spline are extensively used in character recognition techniques [7, 8]. However these are mostly overlooked for signature verification system. Using a shape descriptor solves the problem of size of signature. As Zernike moment returns homogeneous features in polar coordinates irrespective of the size of signature, they are ideally suited for applications where user signature may deviate in size and angle.

One of the most popular features for signature verification system is Zonal or Graph based feature which observes signatures as set of points. It divides the area into zones or grids and estimates different statistics in the zone. Such statistics ranges from local maxima of histograms to local polar or shape features [9-11]. However this technique has certain drawbacks. We have observed that pixel area of signature varies from user to user. While some signatures are really long, some are very short. In a grid based technique, all the signatures must be projected on the grid of same size. Thus Image resizing plays an important role in accuracy of the system. As image resizing is essentially an interpolation, interpolation errors become dominant in such feature descriptor.

Other important group of feature descriptor is moments. Several moments are used in literature for offline signature verification system which includes invariant statistical moments, wavelet moments [12]. Moments are statistics of local or global descriptors of a transform or projection. Hence moment based representation of signatures are popular and efficient.

Radon Transform with Fractal dimension is now other popular feature descriptor for signature verification system [13]. Radon transform proposes a projection histogram over an angle in polar coordinates. Thus signatures are efficiently described using Radon.

Any authentication or verification system can be seen as a pattern recognition problem where the objective is to classify a given pattern (set of features extracted from a test sample) against same features of the samples stored in database. Classifiers are generally divided into two categories: Knowledge based classifier and Regression or Model based classifier.

Neural network and Support Vector machines are very popular classifiers for signature verification system [14]. These systems are first trained by providing a set which contains feature vectors and class id.

Models like HMM and PLS Regression on the other hand are state based models. These techniques consider each sample as an independent entity and generate a rule set automatically. Sample features are classified against stored samples using this rule set. HMM is extensively used in signature verification because of its ability to model an unknown sample as one of the existing samples, PLS is not being used by widely.

### **3. Proposed Work**

A Robust and efficient Signature verification system is important in many applications like banking where personal identification check is associated with economic and other forms of transaction. Even though several Signature verification schemes have already being propose, none of the technique is yet proved to be accurate enough to be accepted with assurance in mission critical applications. Hence there remains a huge potential and scope for this field. Most of the earlier works have focussed signature verification problem as either classification or regression. However if a model or feature set is classified correctly by a classifier, it should technically also be sampled in the same group in a regression model. But as signature sample may involve forgery, a regression may visualize signature indifferently than a classifier. On the other hand if a regression model is used, it needs huge number of samples to actually form the rule set. Number of samples is a big constraint in determining an efficient system with HMM.

In order to overcome this problem, we suggest using Classification-Regression model. A classifier can classify a sample correctly even with lower number of training instances as boundary of each class is defined. Once the sample is classified, a regression model can take all the sample of the recognized class with either one instance from each or training sample or random number of training samples to verify the score weight of the input sample against all

samples. In case the signature is genuine, weight or score of the test sample will be high with recognized class samples than other samples and weights in recognized sample will be similar.

Out of all the classification models SVM is a kernel based classifier which has the capability of rejecting input samples. Kernel projection can be suitably changed and parameters can be adjusted such that the vectors are separable in the feature plane. Hence we use support vector machine.

SVM has other interesting prospect. It is basically a binary classifier. Hence in an authentication system, if the system is supplied with both ID and sample of the test signature, then SVM divides input into two groups: All samples belonging to training classes same as input ID and rest all samples as a single class. On the other hand it can also be made to classify the sample using one against alls classification and returned class can be checked for equality with presented ID. Hence SVM is most suited model for proposed system.

Different feature vectors are proposed by different literature. Radon and Grid based features have found to be most popular. We urge that as signatures are essentially shapes, they are best described by shape descriptor or shape moments. Not many studies are conducted that check the performance of shape based feature in signature verification system. We therefore propose combined shape descriptor of Radon Transform and Zernike moment. The advantage of using both of these descriptors in conjunction is that both the techniques retrieve features from polar coordinates. Hence they represent size and rotation invariant features. Shape features are independent of color model as shapes are extracted either using contours or using edges which are independent of any color model. Thus, these descriptors also solve the problem of background effect in signature verification system.

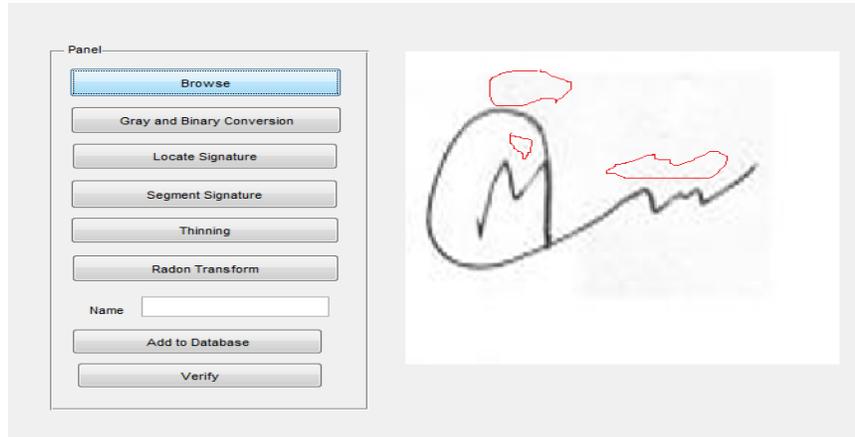
Zonal and Grid features have a limitation in that the signatures must be resized to a predefined window size. Hence short and long signatures suffer from interpolation error. But with proposed descriptors, resizing of the features is not needed as features return unique values for any size.

Detailed methodology is explained in next section.

## **4. Methodology**

### **4.1. Pre-processing**

First step in signature verification system is pre-processing. The need of pre-processing is explained through Figure 1. It can be clearly seen that while scanning a signature on white paper, residues are also scanned. This increases in fuzziness of the pattern. Thus, in the first step such scanning noise must be eliminated.



**Figure 1. Input Signature with Scan Noise**

We perform this by first converting the image to gray scale image. We then convert the image to binary image with a threshold of .7. This results in particularly clear signature pattern as seen in Figure 2.



**Figure 2. Signature pre-processing and Removal of Scanning Noise**

Considering that the signature is scanned against a white background, it can be present at any side of the paper or it can be centralized. Considering this whole image as a sample will lead to improper statistics. Hence ROI of the signature must be extracted first. Many literatures have proposed signature ROI detection using simple bounding box which is demonstrated in Figure 3. This involves two steps: First inverting the signature so that background becomes black and foreground is white and then obtaining a bounding box. However this traditional solution is many limitations when it comes to detecting discontinues signature as shown in Figure 4.

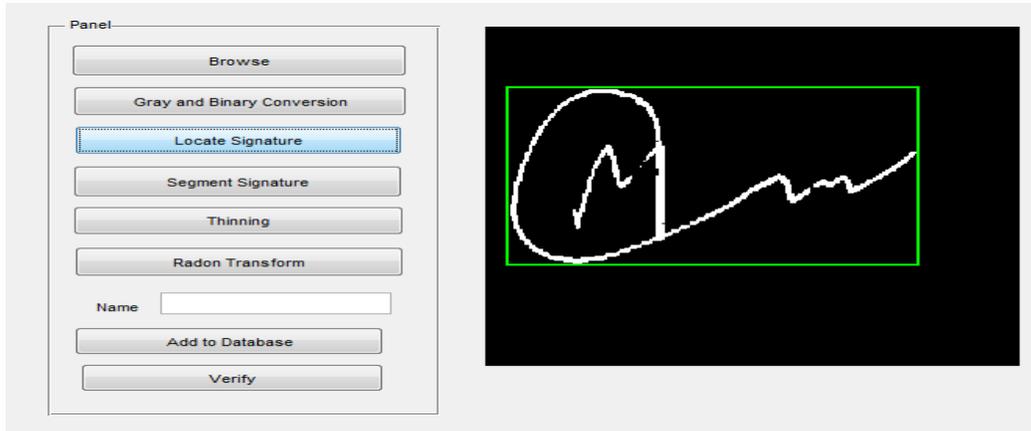


Figure 3. Extraction of ROI of Signature

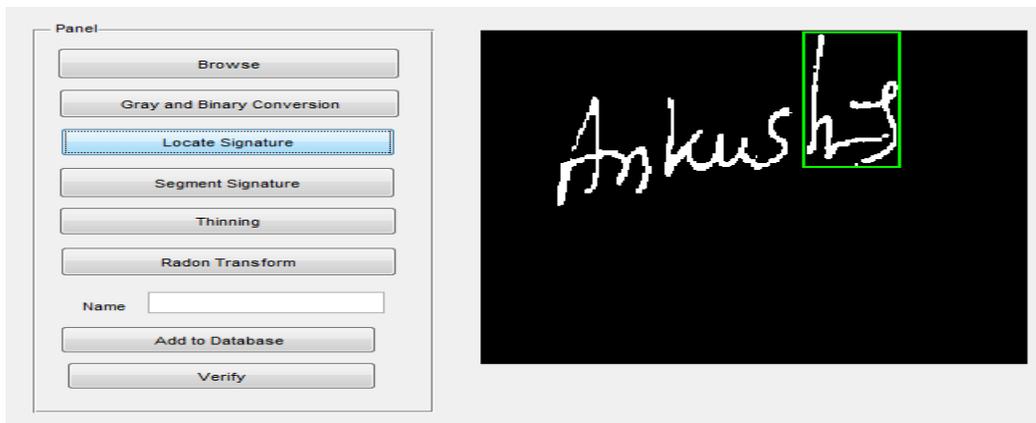


Figure 4. Drawback of Traditional Signature ROI Detection for Disconnected Signatures

This problem is overcome by first dilating input signature with a structuring element of size 16x16 and then applying the bounding box over it. The bounding box region is then annotated over non dilated image to extract the exact region. Results are shown in Figure 5.

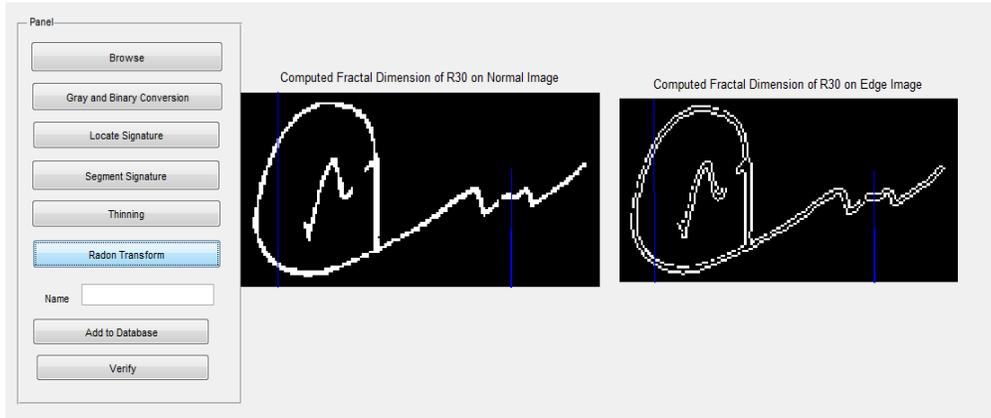


Figure 5. Proposed ROI Detection Technique to Solve Disconnected Signature Problem

Process of binary conversion also results in disconnected lines due to conversion error. This is overcome by first dilating and then eroding the binary image.

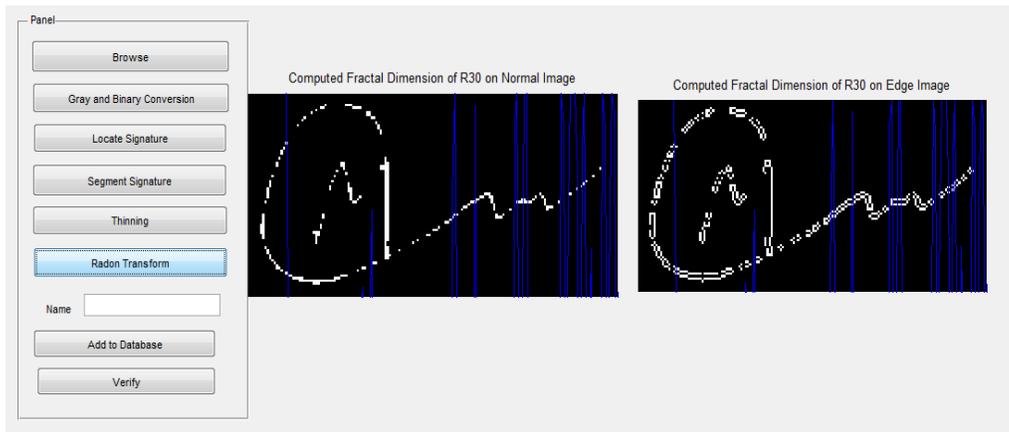
#### 4.2. Feature Extraction

Emphasis of the proposed work is in detecting shape or boundary features. Features can be applied on binary image or thin image or edges. We performed a test to analyse the dominance of features in all three scenarios.



**Figure 6. Feature Extraction from Binary Converted and Edge Detected Images**

Figure 6 reveals that radon features are natural to shapes. Thus descriptors are dominant in same dimension for both normal as well as edge detected images. However number of dominant features is low in both cases. In order to obtain better descriptors we applied thinning with a structuring of kernel 2x2. Results are presented in Figure 7.



**Figure 7. Obtaining Better Feature Descriptors using Thinning Process**

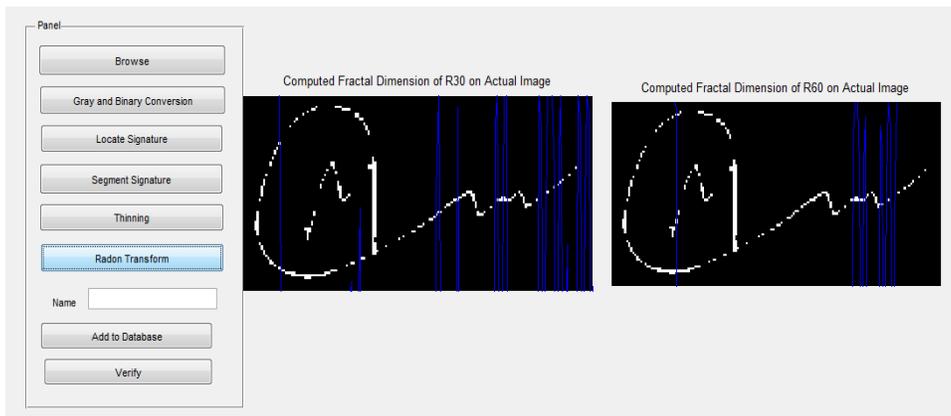
Therefore it is proved that region of interest extraction must be followed by thinning process to extract good descriptor in signature verification system.

Size is another important aspect of signatures. Local feature extraction techniques like Grid/Zone based features extractors demand that all the images be of same size. To study the effect of resizing, we performed feature extraction from resized ROI and without resizing.



**Figure 8. Analysis of Effect of Resizing**

It can be clearly seen from Figure 8 that resizing induces interpolation losses. Hence feature descriptor changes. This leads to misclassification and results in low accuracy. To avoid this problem descriptor must be used on the actual image rather than resized image. However actual image size will vary from one signature to the other. Thus number of descriptors will also vary. One of the prerequisite for any classification is that feature dimensions must be same. Therefore it is wise to extract projection on different angles and extract statistics from them.



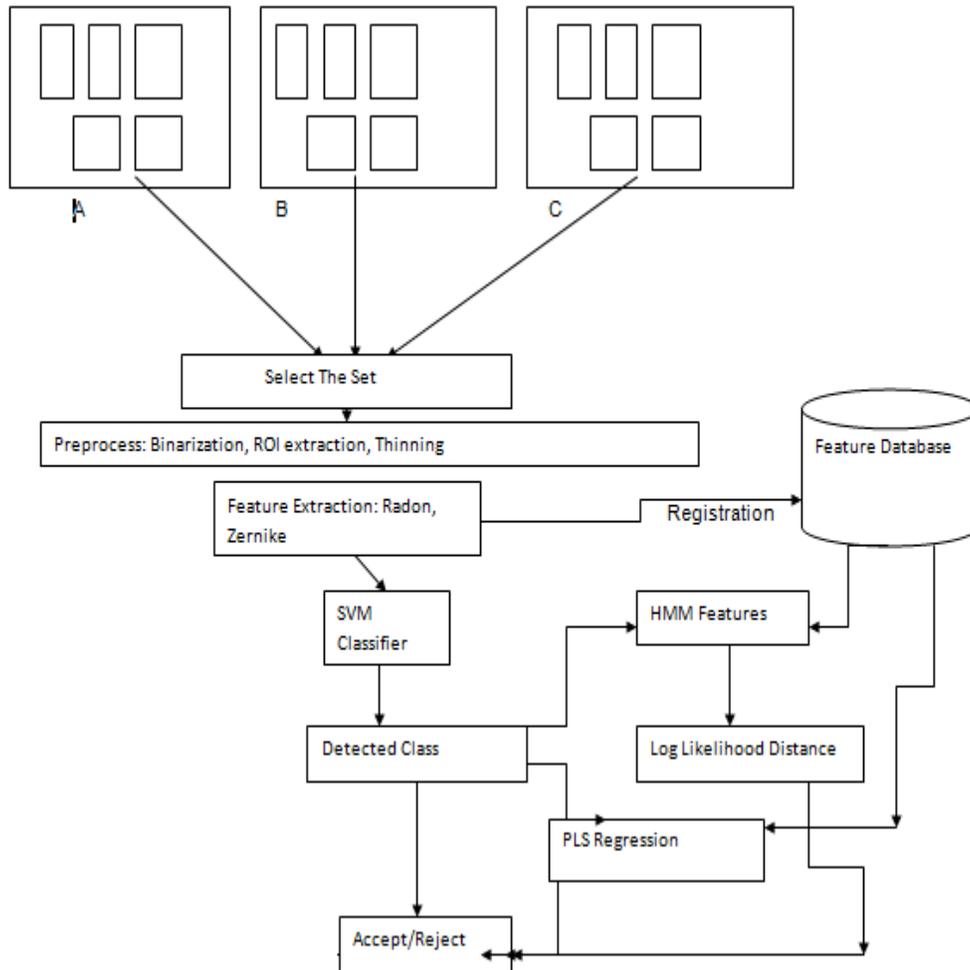
**Figure 9. Feature Descriptor of Radon for 30' and 60' Projection**

It can be clearly seen that the transform descriptors varies as angle of projection varies. It is quite difficult to claim the actual projections that would result in optimized feature set. Hence we obtain Radon descriptors for 0' to 360' in steps of 15' and extract mean and standard deviation for each projection as our Radon feature set.

Once Radon transform is extracted, we obtain Zernike moments before classifying or adding the features to database. Zernike like Radon is a shift invariant moments obtained from polar projection of image. Zernike moments are complex. Therefore real components from the moments are extracted as feature descriptor. Another major limitation of using Zernike moment is that the exponent of the dimension increases as number of moments is increased. But for modelling with HMM, dimensions must be normalized to single value domain. Hence after obtaining Zernike moments we normalize each dimension by dividing it

with the highest exponent of that dimension. Thus all the feature values are brought in same value domain.

Overall methodology is explained with a block diagram in Figure 10.



**Figure 10. Overall Methodology of the System**

## 5. Results and Discussion

Number of features v/s accuracy in FAR and FRR for the proposed system is as shown in Figure 11. It can be seen that FAR is very less in comparison to FRR which is always desirable. Further with increase in features, FAR and FRR both converges to zero. With more features, reparability of the classes is increased. This produces very high accuracy. Number of classes was considered to be 100 for this experiment.

It should be noted that increase in number of classes is expected to degrade the performance of the system to a great deal. However by selecting optimum number of features (500 in this case) leak in accuracy can be prevented. The graph also presents a significant fact that neither SVM nor HMM can expected to be performing optimally when used in isolation. The performance is boosted a great deal when both are used in conjunction.

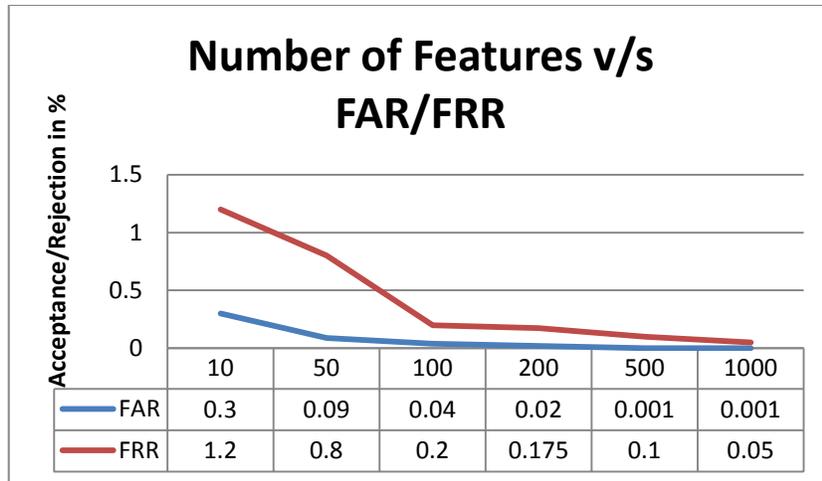


Figure 11. FAR and FRR Performance for Different Numbers of Features

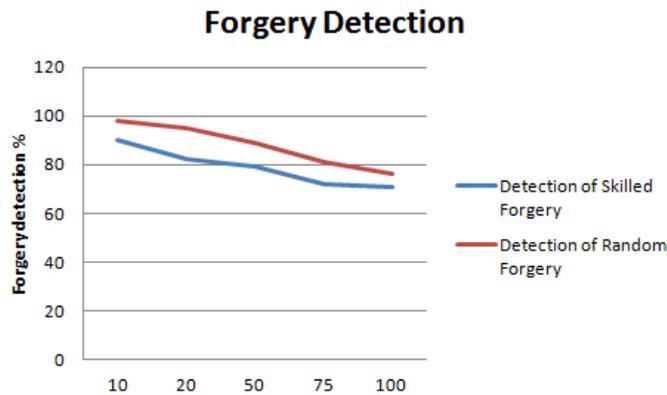
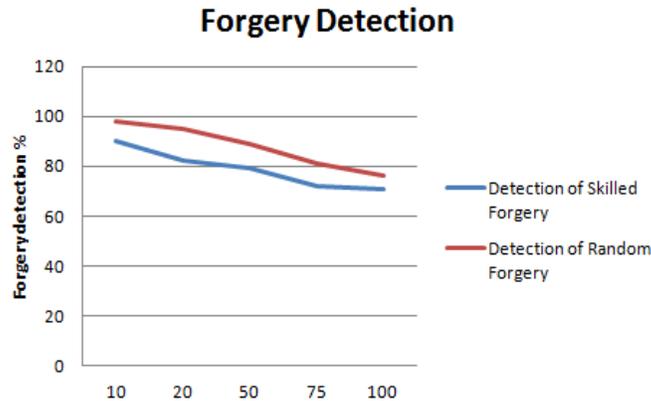


Figure 12. Number of Class v/s Accuracy

Figure 13 represents the performance of proposed system in detecting both skilled and random forgery.

We gathered 50 samples each from 100 users. This set constituted our authentic dataset. We used 10 images for training and remaining 40 image per class for testing. Hence totally 4000 samples were tested for obtaining the accuracy. Expectedly proposed system performed better than independent classifier as presented by figure 12. We have modelled SVM as binary classifier to classify a signature against a given ID. We performed 1000 tests. 500 instances were where we supplied the system with accurate ID and Password. In the second test we supplied the system with wrong but similar signature of the ID. Misdetections is first test false rejection or FRR and the second test are False Acceptance or FAR. It is seen from Figure 12 that FAR is far lower than FRR, proving the acceptability of the system.



**Figure 13. Performance of System in Detecting Forgery**

For testing performance of forgery, we provided 50 users with signature sample of 50 other user. We asked first 50 users to practice the given signature of the given signature pattern to carefully imitate the signature. Every user then produced 10 samples of forged signature. We thus constructed 500 image set of skilled forgery.

We gave the samples of first set of 50 user to second set of user (one user's pattern from first user set to one of the users in the second set). We asked the users to see the sample and produce forged signature, without allowing them to practice. This set of 500 images our test set for random forgery detection.

100 students from 3rd and 4th year of Electronics and Communication Department from SSIT, Tumkur volunteered for this work. Signature patterns were collected on a printed white paper where user put their name, ID and signature in the middle of the page. Users were allowed to use both black as well as blue ink pens. These samples were scanned using a XEROX 3119 digital scanner.

We tested the forgery by supplying a forged signature of a valid ID. Detection is defined as a case when the system rejects the forged signature. The performance is presented in Figure 13. It can be seen that increase in number of classes increases the acceptance of invalid signature. However random forgeries are detected with far better accuracy than skilled forgery. There is still a wide scope of work to efficiently detect skilled forgery.

## 6. Conclusion

Signature verification and analysis are part of larger domain of work which finds application in graphology and forensic science. Signature verification is a challenging aspect as same user's Signature tends to differ depending upon type of Pen being used, the writing surface and so on. Beside, Signature is not considered as unique biometric property. It is rather a pattern associated with different users. Therefore Signature Verification differs from other similar Verification like signature biometric. In this work we have presented a Novel technique of Signature Verification by combining Zernike moments with Radon transform values at different angle of projection from the user's Signature pattern and then forming a statistical state machine with HMM and PLSR. Further the technique was improved by the aid of kernel based techniques with the Help of SVM. As kernel based techniques transforms the training vector to more separable vectors, the accuracy achieved is very high. Results show that cascaded classifier performs better than single stage classifier in both improved accuracy and in detecting forgery.

## References

- [1] A. Al-Omari, "State-of-the-art in offline signature verification system", IEEE, (2011).
- [2] A. Julita, S. Fauziyah, O. Azlina, B. Mardiana, H. Hazura and A. M. Zahariah, "Online Signature Verification System", IEEE, (2009).
- [3] H. S. Yoon, J. Y. Lee and H. S. Yang, "An online signature verification system using hidden Markov model in polar space", IEEE, (2002).
- [4] S. Meshoul and M. Batouche, "A novel approach for Online signature verification using fisher based probabilistic neural network", IEEE, (2010).
- [5] M. J. Alhaddad, D. Mohamad and A. M. Ahsan, "Online Signature Verification Using Probabilistic Modeling and Neural Network", IEEE, (2012).
- [6] M. I. Malik, S. Ahmed, A. Dengel and M. Liwicki, "A Signature Verification Framework for Digital Pen Applications", IEEE, (2012).
- [7] C. Singh, E. Walia and N. Mittal, "Rotation invariant complex Zernike moments features and their applications to human face and character recognition", IEEE, (2011).
- [8] C. Kan and M. D. Srinath, "Combined features of cubic B-spline wavelet moments and Zernike moments for invariant character recognition", IEEE, (2011).
- [9] A. C. Ramachandra, K. Pavithra, K. Yashasvini, K. B Raja, K. R. Venugopal and L. M. Patnaik, "Cross-validation for graph matching based Offline Signature Verification", IEEE, (2008).
- [10] S. Chen and S. Srihari, "A New Off-line Signature Verification Method based on Graph", IEEE, (2006).
- [11] S. Srivastava and S. Agarwal, "Offline signature verification using grid based feature extraction", IEEE, (2011).
- [12] A. I. Al-Shoshan, "Handwritten Signature Verification Using Image Invariants and Dynamic Features", IEEE, (2006).
- [13] J. Coetzer, B. M. Herbst and J. A. du Preez, "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model", EURASIP Journal on Applied Signal Processing, (2004).
- [14] S. F. Miskhat, M. Ridwan, E. Chowdhury, S. Rahman and M. A. Amin, "Profound impact of artificial neural networks and Gaussian SVM kernel on distinctive feature set for offline signature verification", IEEE, (2012).

## Authors



**K. N. Pushpalatha** is an Assistant Professor, Department of E&C, Dayananda Sagar College of Engineering, Bangalore. She obtained B.E degree in Electronics & communication from Bangalore University and M.S. Degree in Electronics and Control from BITS Pilani. She is pursuing her Ph.D in Electronics at Mewar University, Rajasthan under the guidance of Dr. Arvind Kumar Gautham, Principal, S D College of Engineering, Muzaffarnagar, Uttara Pradesh. Her research interests include Image Processing, Biometrics, Information Theory and Coding.



**Arvind kumar Gautam**, is working as principal of S.D. college of Engineering and Technology, Muzaffarnagar, Uttara Pradesh. He received his M Sc degree in physics from Meerut University, M Tech Degree in Instrumentation from Regional Engineering College, Kurukshetra and M Tech. Degree in Electronics and communication from JNRV University, Udaipur. He has obtained Ph.D. degree in Physics from Meerut University. He has got 31 publications in national and international conferences. He has published two books in Antenna and Wave Propagation and Electromagnetic Field Theory. He is also the author for two Text books of physics.



**Shashikumar D R** received the BE degree in Electronics & Communication Engineering from Mysore University and the ME degree in Electronics from Bangalore University, Bangalore. He is pursuing his Ph.D. in Information and Communication Technology of Fakir Mohan University, Balasore, Orissa. He is currently working as Professor, Dept. of Information Science and Engineering, Cambridge Institute of Technology, Bangalore. His research interests include Microprocessors, Pattern Recognition, Biometrics, Digital Image Processing, and Computer Networks.



**Dr. ShivaKumar K B** received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA from Bangalore University, Bangalore and M Phil from Dravidian University, Kuppam. He obtained his Ph.D. in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 50 publications in International journals and conferences. He is currently working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, Multi rate systems and filter banks and Steganography.



**Rupam Das** received his BE degree in Electronics and Communication from VTU, Belgaum in 2002 and M. Tech degree in Computer Science and Engineering from VTU, Belgaum in 2012. He is founder and CEO of Integrated Ideas, a R&D firm in Gulbarga, Karnataka. He is also heading the R&D department of the company. He has over 10 publications in reputed international journal and conferences. He is known for his contribution in Intel perceptual computing and has won three top prizes in perceptual computing challenge. His area of interest is robotics, perceptual computing, biometrics and wireless networks.

