

ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

Offline Signature Recognition and Verification System using Optimum Hybrid and Texture Features

¹Dr Ramya Rani N,

¹Assistant Professor, Department of Electronics and Communication Engineering, V.S.B. College of Engineering Technical Campus, Coimbatore, Tamil Nadu, India

E-mail: ¹ramyaranivsb@gmail.com

ABSTRACT

The proposed offline signature recognition and verification system is analyzed for a database of 196 signature images that includes standard databases and real time signatures. Extraction of appropriate features from images and selection of best features play an important role in increasing the accuracy rate of signature recognition and verification. In this work, two categories of features set are extracted namely hybrid features set (global, local, texture feature using GLCM) and texture features set using GLDM and Haar wavelets only. The optimum features are selected separately from both the feature sets using genetic algorithm. The accuracy rate of identification and verification of signatures based on both the optimum feature sets are analyzed using Support vector machine, Artificial Neural Network and Naive Bayes classifiers. The simulation results show that, compared with Support Vector Machine (SVM), artificial neural network and Naive Bayes classifier provides better signature recognition rate and accurate results in verifying the signatures of the created database. In the existing work, 67% of verification accuracy rate is achieved using Random forest classifier for 20 signatures from ICDAR 2009 database. Compared to this existing work, the proposed system increases the accuracy rate to 94% using SVM Radial Basis Function kernel for the 120 signatures considered from the same ICDAR 2009 database.

Keywords: Biometrics, feature extraction, feature selection, signature recognition and verification, machine learning algorithms

1. INTRODUCTION

In present scenario, identification and authentication of person is an important area of research in various fields like banking transactions, document authentications, credit card receipt, electronic funds transfer electronic commerce and other high security environments [1]. Traditional method of personal identification by PIN (Personal Identification Number), passwords may be easily forgotten and recognizing with passports, driving licenses and voter ID (Identity) card may easily be forged. Thus biometric method of personal identification came into existence and gained importance over the traditional methods [2]. Individual biometric characteristics are not easily transferred, stolen or lost and hence it gain advantage over the other authentication methods like PIN numbers, passwords and smart cards.

Biometrics is a science that examines the physiological and behavioral characteristics for verifying the person identity. Biometrics is classified into two major categories namely physiological and behavioural biometrics. The authentication of an individual based on physiological characteristics include facial recognition, finger print recognition, hand geometry, retinal scanning and iris recognition. Signature, voice and keystroke are the behavioural biometric characteristics for person identity. Personal

authentication becomes a major factor in all areas of applications[3].

Even though many forms of authentication are available in today's world, signature biometrics is a socially accepted method of authentication in all banking applications. Signature is a behavioral biometric that has high time variability compared to other physiological biometrics. Online signature recognition and verification system requires electronic tablets, stylus for acquiring the signatures and hence found to be more expensive than offline signature recognition and verification system [4].

IoT is an efficient platform to implement a low cost secured biometric system. IoT is the recent wireless technology that connects many embedded devices simultaneously through internet. The information is exchanged among the connected devices confidentially and provides a secured biometric system. The security and the efficiency of the signature verification system can be enhanced using block chain technology [5].

2. LITERATURE REVIEW

Recent research works acquired signature images from ICDAR [6], MCYT-75[7], GPDS-300[8], SVC2013 [9] and SVC20EU [10] signature databases for verifying genuine and forged signatures. Ferrer et.al [11] designed the offline



ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

signature verification system on gray level feature extraction and provided better performance in verification. More accurate results in determining signature forgeries are obtained in local grid based feature extraction proposed by [12] and [13]. In major works by [14] and [15], global and local feature extraction provides increase in accuracy rate for classifying the genuine and forged signatures.

Some of the works proposed in [16] and [17] texture features are extracted for the signatures in a dataset and classified using support vector machine and Neural network respectively. In all the above works, the performance metrics provides comparatively less error rate in verifying signatures using either global or texture features or global and local features.

The selection of optimum features for signature identification and authentication provides the accurate results at a faster rate. Various algorithms like Principle Component Analysis (PCA), Partial Least Square (PLS), genetic algorithm [18] and Probabilistic Neural Network based Artificial Bee Colony (PNN-ABC) algorithm have been utilized for feature selection in signature verification system. Compared to other algorithms, selection of optimum feature using genetic algorithm provides faster accurate results and retain the original information of the extracted features [19].

In the context of offline signature verification, it discusses two primary approaches: writer-dependent and writer-independent methods. Additionally, the study includes an analysis of feature extraction and classification techniques employed in the signature identification and verification process. Various databases referenced in the literature are utilized to assess different signature identification and verification techniques, with the corresponding results detailed in this article. The entire review is further encapsulated in a comparative table. To highlight the advantages of this survey, a comparison with recent existing surveys is also provided. Lastly, the paper outlines potential future research directions[2].

Many machine learning algorithms have been utilized for training and testing the extracted features for signature verification system. Machine learning techniques are classified into supervised and unsupervised learning. Supervised learning works with known input, predicted output responses and provide accurate results in classifying the data. Some of the supervised learning techniques are K nearest neighbor (KNN), Multilayer Perceptron (MLP), dynamic time warping (DTW), neural network, Naive Bayes classifier, Hidden Markov Models (HMM) and support vector machines (SVMs) [20]. Recent works on signature verification system utilizes among these machine learning algorithms for classifying genuine and forgery signatures. These supervised techniques have its advantages, limitations as stated in and provides accurate results depending on the signature dataset.

Table 1 Literature based on related work

Table 1 describes the survey of recent research works in

Refer ence	Work Contribution	Outcomes
[2]	Survey of writer – dependent and writer independent approaches of offline signature verification system	Many feature extraction and classification techniques for many databases are presented. Comparison of existing work for future research are also presented
[21]	Alex Net and transfer learning architecture are incorporated for the verification of simple and skilled forged signatures.	Feature extraction is improved with the extraction of brush stroke. Transfer learning architecture is used with small number of samples. The recognition rate is 95.63% for the detection of skilled forgeries.
[27]	Gaussian filter is utilized in the preprocessing stage of the system. GLCM (gray level cooccurrence matrix) feature extraction technique and kernel principal component analysis are utilized for the classification stage using machine learning algorithms.	The system achieved accuracy of 56.66% for Naive Bayes algorithm, 82% for K-Nearest Neighbour (KNN) and 81.66% for Random Forest using principle components.
[28]	Convolution Neural Network, Recurrent Neural Network and Dynamic Time Warping are utilized for the signature databases to determine the signature forgeries.	System performance is improved
[29]	The two-stage Siamese network model is implemented with an efficient spatial transformation network and the Focal loss functions overcome the imbalance between positive and negative signature images.	The proposed work outperforms the existing work in terms of verification accuracy.
[30]	The signature identification is based on the integration of dynamic and static feature extraction. Chinese signature database is used for the detection of signature forgeries.	The obtained integration of effective features provides better accuracy compared to other works.

signature recognition and verification system based on feature extraction and machine learning algorithm.

1.1 Research Motivation and objectives



ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

Compared to online signature verification, offline signature verification is more challenging because imitating the users' offline signatures are simple in real life situations. In offline signature recognition and verification system, major research works have been carried so far, but still many challenges exist in the selection of best features, in recognizing the signature variations of the same user and in reducing the signature forgeries

These aspects motivated the research work to focus on the following objectives:

- To extract and fuse global, local and texture features
- To select the optimum features from the extracted features using genetic algorithm.
- To recognize and verify the user's signatures based on optimum selected features using Support Vector Machine, Artificial Neural Network and Naive Bayes classifiers.

1.2 Overview of Proposed work

In the proposed work, a database of 196 images are focused in extracting global, local, texture features and fusing all the three categories for extracting features of all the images in the database. Genetic algorithm has been utilized to select the optimum features from the extracted features. Majority of the survey works of offline signature verification system shows only the results for authenticating the user's signature. Many time people's signature may vary due to aging, illness, speed of signing and the same person's signature may not look alike when the original signature sample was taken to store in a database. To overcome this limitation, the proposed work is focused to identify the owner of the signature and then to verify their originality using Support Vector Machine (SVM), artificial neural network and Naive Bayes Classifiers based on the selected features. The selection of proper kernel functions decides the accuracy of the system in SVM and hence in this work, the support vector machine classifier is focused to analyze for linear kernel and Radial Basis Function (RBF) kernel functions.

The paper is organized as follows: Section 2 describes the pre-processing and feature extraction stages of the system. Section 3 discusses the feature selection using genetic algorithm. Section 4 details the signature recognition and verification using support vector machine, artificial neural network and Naive Bayes classifiers. Section 5 details the performance metrics of the proposed system. Section 6 concludes the work with future scope.

3. PRE-PROCESSING AND FEATURE EXTRACTION

3.1 Data Acquisition

In this work, possible signature images are obtained from TC11 ICDAR 2009 database consisting of genuine and forged signatures. The forged signatures in this database were

collected by skilled forgers [6]. From this database, 60 genuine signatures and 60 forged signature variation images contributed by 12 genuine persons are considered for the research work. Similarly, 45 signatures are obtained from the SVC20EU/SVC2004 dataset website consisting of 30 genuine signatures and 15 forged signatures contributed by 3 users [10].

In addition to these signatures from standard databases, 31 real time genuine signatures are included in genuine signature database for recognizing the signature variations of the same genuine users. Thus the created database consists of 121 original signatures, 75 forged signatures and hence, a total of 196 signature images are considered for signature recognition and verification.

3.2 Pre-Processing

The 196 signature images in the database obtained in the data acquisition stage have been considered for preprocessing the images. The gray scale or colour images are read from the database as a string file. The signature images in the dataset are of in different size and shape. Hence the images are resized to a standard size of 256×256 as shown in Figure 1.



Figure 1 Sample resized input images

Then the images are checked for colour or gray scale images based on the dimensions of the signatures. If the dimension of the images read greater than or equals 2, then the colour image is transformed into gray image. This conversion has been performed in MATLAB based on the equation (1).

$$0.2989 \times R + 0.5870 \times G + 0.1140 \times B$$
 (1)

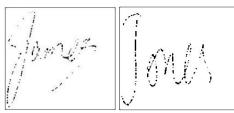


Figure 2 Filtered images

The gray scale images are further binarized and thinned using morphology operation to get the proper geometric shape of the signature. Thinning process removes the pixels of the text contour by retaining one pixel width. The thinned signature images are further filtered using median filter to remove salt and pepper noise of the images as shown in figure 2

ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

3.3 Feature-Extraction

This section describes the extraction of global, local and texture features.

3.3.1 Global features

In this work, global features like area, length, width and Histogram of Gradients (HOG) have been extracted for signature verification. Signature area represents the number of pixels belonging to the signature. The size of the images represents the length and width of the image in two dimensions. The histogram indicates the pixel intensity values. It refers to the number of pixels at each intensity value of an image. This was introduced by Dalal and Triggs in 2005[22]. The Histogram of Gradient (HOG) feature determines the appearance of the number of oriented gradients in the region of interest (ROI). The HOG algorithm computes the gradient directions, magnitudes, forms the cell histogram based on oriented gradients and determines the average of the normalized histogram.

3.3.2 Local features

In this work, local features like number of black pixels, slant angle, grid feature, centroid and orientation features have been extracted for verifying the signature images in the classification stages. The total number of black pixels of the image is calculated from the pre-processed filtered image by excluding the pixel with '0'binary value.

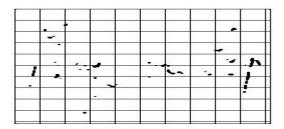


Figure 3 Signature grid images

Figure 3 shows the sample images of the signature overlaid on the grid. Rectangular grid (10×10) is formed by dividing the image into 100 square cells at a spacing of 25 between each cell. The number of black pixels is calculated in each rows and columns of the cell. The normalized value of minimum number of black pixel rectangle is '0' and the maximum number of black pixel rectangle is '1'. The total normalized values represent the grid feature vector. The formation of grid cells captures both global and local features of a signature. The local histogram features, distribution of edges within each cell and the detection of line segments are extracted from each cell or within the grid region. The histogram of local binary patterns within each grid cell can also be captured using the pixel intensities.

The slant angle is computed based on radon transform of the image. The Radon transform(R) of an image is the sum of the radon transforms of each individual pixel. The radon transform between the filtered image and the theta angle returns

a numeric vector xp (367×1 double) containing the radial coordinates corresponding to each row of R. The radial coordinates returned in xp are the values along the x'-axis which is oriented at theta degrees counter clockwise from the x-axis. The columns of R contain the Radon transform for each angle in theta. The slant angle is computed from the mean of the maximum column value of R of the Radon transformed image.

Centroid is defined as the centre of the horizontal and vertical point of the signature. Here centroid, a one by Q vector is calculated from the region properties of the image. Q represents the number of image dimensions. The first element of centroid is the horizontal 'x' coordinate and second element is the vertical 'y' coordinates. All other elements are in the order of image dimensions. The mean of orientation features is obtained with the rotation of pre-processed filtered images from 90° to -90° .

3.3.3 Texture features

In this work, texture features are extracted using GLCM, GLDM and Haar wavelets. Gray level co-occurrence matrix (GLCM) or Gray level spatial dependence matrix examines the structural and spatial properties of the image texture. GLCM is a matrix that determines the occurrence of gray level pixels with intensity 'i' adjacent to a pixel with intensity 'j'. This spatial relationship called pixels of interest is equal to the number of rows and columns of the gray scale image. The number of gray levels in the image determines the size of the GLCM. The adjacent pixels can be defined in any of directions of 0°, 45°,90° and 135° when the image is transformed into GLCM matrix [23], [24]. In this work, mean, contrast, energy, correlation, maximum probability and homogeneity features are extracted from the signature database.

Mean (μ) value measures the average intensity of the image. Contrast (C) measures the local variations in the gray level co-occurrence matrix based on the pixel intensity and its neighbors of the image. The contrast value is high for uniform gray levels of the image. Energy (E) provides the sum of squared elements in the GLCM. It is also called as angular second moment or uniformity. Energy is high for similar pixels of the image. Correlation (Co) measures the joint probability occurrence of the specified pixel pairs based on the gray levels of the image. This parameter provides image tracking methods for measuring the image changes with high levels of accuracy for two dimensional and three dimensional images.

Correlation parameter measures the motion of optical mouse, displacement, elasticity and used in engineering and science applications [24]. Homogeneity (H) is a measure of very few gray levels of the image with high values of M (i,j) for homogenous images (i=j). This parameter is also called as inverse difference moment. Maximum probability is a measure of largest value of M (i, j) in the centre pixel of the image window. Maximum probability occurs when one pixel pair dominates the other pixel pair in the image. In this work, the average of the maximum probability value is computed as a feature for each of the image.

➤ Gray Level Difference Method (GLDM)

ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

Gray Level Difference Method (GLDM) estimates the probability density functions for a pre processed image. In this work, four probability density functions (pdfs) of the filtered image have been estimated for extracting the texture features of the image. Initially the four pdfs for the inter sample distance 'd' (0,d,-d,d,d,0,-d,d) have been assigned to zero. The absolute differences between the central pixel and images at top, down, left and right direction have been computed. Then 4 probability density functions have been estimated for the gray level images with the intensity range of (0-255) in all the four directions. The histograms of the probability density functions have been estimated. The mean and standard deviation features are extracted from each of the cumulative sum of histograms of the probability density functions.

➤ Haar wavelet

In this work, Haar wavelet is applied on the gray scale image. Using 2-D discrete wavelet transform, the grayscale image is decomposed into four sub band frequency levels namely Low Low (LL) frequency, Low High (LH), High Low (HL) and High High (HH) frequency levels. The DWT transform returns the coefficients for each of the frequency levels. The Low Low (LL) frequency band provides the approximate image compared with the remaining sub band frequency levels [23]. Hence LL sub band is further decomposed into 4 sub bands namely LL₁, LH₁, HL₁ and HH₁. The mean feature is extracted from the LL₁ frequency band of 2^{nd} level decomposition of Haar wavelets.

4. FEATURE SELECTION USING GENETIC ALGORITHM

Figure 4 shows the genetic algorithm for selecting the best features from the extracted features of the images. The population size is initialized as '20' for hybrid features, '9' for texture features of bit string type and the maximum number of generations or iterations count as '50'. Population size indicates the number of individuals or chromosomes in each generation. The increase in population size reduces the computation speed of the algorithm. The bit string population type specifies the individuals in the population have '0' or '1' component value. Initially population function of individuals is randomly generated within the range of 0 to 1. These randomly generated population values are stored in a variable. Then the random values are generated based on the initialized population size '20', genome length '17' for hybrid features and '9' for texture features.

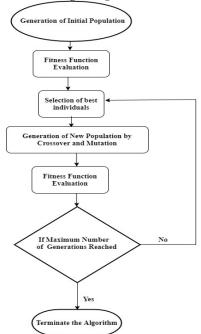


Figure 4 Flowchart for feature selection

The initially created population matrix of dimension $20{\times}17$ and $9{\times}9$ is applied separately to fitness function evaluation of hybrid and texture features respectively. The chromosomes with value '1' are selected from the population function and it indicates the feature index. The fitness function is an objective function to compute the discriminative capability of the extracted feature set. This function is evaluated based on K-Nearest Neighbour (K-NN) classifier.

The fitness function is computed based on resubstitution loss of K-NN classification, number of original extracted features and number of selected feature index values as in equation (2). The resubstitution loss function calculates the classification loss or error using the training data and class labels of K-NN algorithm.

Fitness Function=
$$\frac{\beta}{N_{F-N_S}}$$
 (2)

Where β = K-NN classification loss error N_F = number of original features.

Based on fitness ranking, the selection function selects the best two chromosomes from the population excluding the elite children. This process is continued iteratively till the filling up of new generation of population.

In this work, the maximum numbers of generations limits and stall generations limit is set as '50'. The algorithm analyse the average difference of best fitness values of all generation of chromosomes. The algorithm stalls, when the average relative difference of fitness values of 50 generations over stall generations is less than or equal to function tolerance value of 0.000001.

At the end of iteration, based on the fitness function evaluation and 17 number of hybrid features, best chromosomes are obtained. The chromosomes with binary value '1' are computed



ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

as the best chromosomes and thus the 5th (correlation),13th(centroids) and 14th (HOG) features in order are selected as the best hybrid features from the hybrid set. Similarly, the 9 texture features in order are 4 mean values, 4 standard deviation values of probability density functions and low-low level (LL) of Haar wavelet. The chromosomes with binary value '1' are computed as the best chromosomes and thus the 9th feature (LL) in order is selected as the best texture feature from the texture feature set.

5. SIGNATURE IDENTIFICATION AND VERIFICATION

5.1 Support vector Machine

Support Vector Machine (SVM) is a binary linear classifier and the learning process is based on statistical learning theory. The classification is based on determining the optimum separation hyperplane in the feature space. The selected features of 196 images in the database are used as predictors in SVM training and classification. The dimension of input data features (x) is 196×3 for optimum hybrid feature set and 196×1 optimum texture feature set. The target output data is 32×196. It has been proved that compared with other kernel functions, RBF kernel provides increased accuracy rate [25]. Hence in the proposed work, recognition and verification of signatures are analyzed for both linear and RBF kernel functions of support vector machine. The Error Correcting Output Code (ECOC) multiclass label is trained with selected optimum features(x), 32 class labels(y) of 196 images and binary learners with kernel functions using one versus one (OVO) coding design. The number of binary learners is 17×136 for optimum hybrid feature set and texture feature set. The OVO coding design maps each of the binary learners with one class as positive, other class as negative and remaining classes are ignored. The trained ECOC model returns the structure with 17×1 cell array of owner's name, support vectors, alpha, bias, μ and σ for each of the binary learners. The test signature features are predicted with the target data of trained ECOC model. The column of the test signature features are standardized with the mean (μ) and standard deviation (σ) values of trained classifier. Similarly, the optimum features and target data of 2 class labels are trained and tested using SVM for signature verification.

5.2 Artificial Neural Network

The feed forward neural network architecture is created with input layer, hidden layers, training algorithm, activation function and output layer. The input layer receives 3 inputs (hybrid features) and 1 input (texture feature) based on the type of optimum features selected for creating the neural network. Thus, for the identification and verification of signatures, the dimension of optimum input data is 196×3 and 196×1 for creating neural network. The target data is 32 class labels to identify the user names of 196 signature images and 2 class labels to verify the originality of the identified user's signatures. The dimensions of output data is 32×196 and 2×196 for signature identification and verification respectively. Based on the input data and output data, 30 units are initialized for

each of the 2 hidden layers. Hyperbolic tangent sigmoid activation function is used as a transfer function for transforming the information from the input layer to each of the hidden layers and is computed as shown in equation (3).

$$= \frac{2}{1+e^{-2n}} - 1 \tag{3}$$

The created neural network is trained with the optimum selected features and 32 class labels using Levenberg Marquardt back propagation learning algorithm for signature recognition. The main advantage of Back propagation algorithm is the output values greater than the error level is fed back to the input layer for further updation in bias and weight values [26].

The trained network is simulated with test data features. The simulation of the neural network depends on the properties of number of layers, number of inputs, number of output and the weight values that connect the layers. Based on these properties, the simulation of neural network applies weight and bias values to the input data features to obtain the output at each layers of the neural network. The simulation results are rounded off to the nearest integer(x). Similarly, the trained network is classified by simulating the network with test data features and the results are rounded off to the nearest integer(x) with dimensions 2×196 . The output is classified as original signature when x (1, 1) is '1' and when x (2, 1) is '1' the output is classified as forged signature. The output of all signature images in the database is saved as a string of dimension 196×1 .

5.3 Naive Bayes Classifier

Naive Bayes classifier is a supervised learning algorithm for pattern classification problems based on statistical analysis. It is used for the predictor input data that are assumed to be independent with each of the class labels. In this work, the Naive Bayes algorithm initially assumes the predictor data features (j) to be conditionally independent within the class labels. The dimension of the predictor data features (j) is 196×3 for optimum hybrid features and 196×1 for optimum texture features. 196 images are grouped under 32 class labels of 17 unique names for identifying the owner of the signature and grouped under 2 class labels for verifying the signatures. The training function is initialized with predictor data features, respective class labels and multivariate multinomial distribution function.

The trained naive bayes model is classified with the test data features(X) and all data features(X) to predict the class labels for signature recognition and verification. The output is returned as a character array of 196×1 of all signature images in the database for both recognition and verification. The predict classification results are also returned as posterior probabilities and expected misclassification costs for each of the observations in class 'k'. In the testing stage, floating point double valued posterior probability function matrix and misclassification cost matrix of dimension 196×17 for signature recognition and 196×2 for signature verification is obtained.

ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

The observation that belongs to the particular class label is also classified based on the maximum value of posterior probability function and the minimum value of expected misclassification cost.

6. PERFORMANCE METRICS ANALYSIS

6.1 Signature Recognition Results

Table 2 Signature recognition based on optimum hybrid features

Table 3 Signature recognition based on optimum texture features

Parameters	SVM Linear Kernel	SVM RBF Kernel	Artificial Neural Network	Naive Bayes
Correct recognition Rate %	41.83	46.40	40.62	98.40
Positive Predictive Value %	38.23	40.54	98.70	93.75
Negative Predictive Value%	98.70	100	84.70	100

Table 2 shows the signature recognition results using the three classifiers based on the selected hybrid features. Correct recognition rate specifies the percentage of correctly classified samples. Positive predicted value denotes the

Parameters	SVM Linear Kernel	SVM RBF Kernel	Artificial Neural Network	Naive Bayes
Correct recognition Rate %	72.9	92.8	92.8	100
Positive Predictive Value %	81.25	100	98.9	100
Negative Predictive Value%	98.8	99.4	0	100

percentage of correctly classified positive samples and negative predicted value denotes the percentage of correctly classified negative samples. From the table, it is clear that 100% of accuracy is achieved using Naive Bayes classifier in recognizing the owner of the signatures in the considered database compared with SVM and artificial neural network.

Table 3 shows the signature recognition results of all 196 images in the database classified through the 3 classifiers based on the selected texture features. Compared with the 3 classifiers, 98.4% of accuracy is achieved using Naive Bayes classifier in identifying the signatures correctly based on texture features. However, the percentage of identifying the correctly classified positive signatures is high for artificial neural network classification. Comparing the performance of linear and RBF kernel of SVM, classification based on RBF kernel functions provided better performance metrics.

6.2 Signature Verification Results

Table 4 shows the performance metrics of signature verification of all 196 images using SVM, ANN and Naive Bayes classifiers based on the selected hybrid features. From the table it is clear that, 93.3% of accuracy is achieved in both artificial neural network and Naive Bayes classifier. However, comparing the other parameters, one classifier outperforms the other classifier. The percentage of accepting genuine signatures is more in Naive Bayes classifier and the percentage of rejecting forgery signatures is high using artificial neural network. Similarly, the percentage of accepting forgery signatures is more using artificial neural network and the percentage of rejecting genuine signatures is high in Naive Bayes classifier. Comparing the performance metrics of linear SVM and RBF kernel SVM, SVM classification using RBF kernel provided better signature verification results.

Table 4 Performance analysis of classifiers based on optimum hybrid features

Parameters	SVM Linear Kernel	SVM RBF Kernel	Artificial Neural Network	Naive Bayes
Accuracy	61.70	83.10	93.36	93.33
Sensitivity	100	90.00	95.86	90.00
Specificity	0	72.00	89.33	98.60
TRR	NAN	81.80	93.05	86.00
FAR	100	28.90	11.84	02.63
TAR	61.40	83.20	92.80	98.10
FRR	0	09.91	04.13	09.91

Table 5 Performance analysis of classifiers based on optimum texture features

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

Parameters	SVM Linear Kernel	SVM RBF Kernel	Artificial Neural Network	Naive Bayes
Accuracy	61.70	64.70	93.30	93.33
Sensitivity	100.00	78.50	97.52	99.17
Specificity	0	42.60	86.60	84.00
TRR	NAN	55.10	95.58	98.40
FAR	100	57.80	14.40	17.10
TAR	61.40	68.30	91.47	90.22
FRR	0	21.40	02.47	0.82

Table 5 shows the performance metrics of the verified 196 signatures using the classifiers based on the selected texture features. From the table, it is inferred that Naive Bayes classifier and artificial neural network provides accurate classification results compared with SVM. The performance of artificial neural network and Naïve Bayes classifiers are viceversa in terms of FAR, FRR, TAR and TRR metrics.

The proposed signature verification system is compared with an existing work of offline signature verification system based on the number of signature samples, feature extraction and classification techniques.

Table 6 Performance comparison of classifiers for ICDAR 2009 signatures

Signature Verification Accuracy Rate % (Existing work)		Signature Verification Accuracy Rate % (Proposed work)	
Multinomial Naive Bayes classifier	40	Linear SVM	75.83
Logistic Regression classifier	53	RBF kernel-SVM	94.16
Stochastic Gradient Descent & Random Forest classifier	67	Artificial neural network	93.3

Table 6 shows the comparison results of the proposed system with an existing work. In [6], out of 1953 signatures, 20 signature samples of original and forged images were acquired from ICDAR 2009 [21]. In this work, shape and pixel features were extracted and analyzed using Multinomial Naive Bayes classifier, logistic regression, stochastic gradient descent and random forest classifiers. The performance analysis using random forest classifier and Stochastic Gradient Descent classifier showed an accuracy rate of 67% compared with other

classifiers. Compared to this work, the proposed research work achieved an accuracy rate of 94.16% using Radial Basis Function kernel of Support Vector machine classifier by selecting optimum hybrid features. The proposed work is analyzed for 120 signatures from ICDAR 2009 database.

7. CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

The proposed work is focused on the identification of the owner and verification of the originality of 196 images of genuine and forged signatures in a database. The best optimum features of the signature images are selected by genetic algorithm for two feature sets. The selected best features in both the sets of all the signature images had been trained and tested separately using linear Support Vector Machine (SVM), Radial Basis Function kernel SVM, Artificial Neural Network (ANN) and Multivariate Multinomial Naive Bayes classifier. The performance metrics of the classifiers is analyzed separately for optimum hybrid features and texture features. From the analysis, it is concluded that Naive Bayes classifier achieved 100% correct recognition rate for optimum hybrid features and 98% correct recognition rate for optimum texture features set compared with other classifiers.

The performance analysis of signature verification using Naive Bayes classifier and artificial neural network achieved an accuracy rate of 93% based on both optimum hybrid and texture feature set. The achievement of same accuracy rate in Naive Bayes classifier based on optimum hybrid and texture features is analyzed further in terms of FAR, FRR, TRR and TAR performance metrics. Based on the analysis of these parameters, it is concluded that the performance metrics of optimum hybrid features was inversely proportional to optimum texture features in Naive Bayes classifier.

The proposed system is compared with an existing signature verification system classified using Multinomial Naive Bayes classifier, Random forest classifier, stochastic gradient descent and logistic regression classifier. This system achieved an accuracy rate of 67% using Random forest and stochastic gradient descent classifier for classifying 20 samples of ICDAR 2009 database of signatures. Compared to this work, the proposed system showed 27% increase in accuracy rate using Radial Basis Function kernel of Support Vector machine. The proposed system verified 120 signatures from the same ICDAR 2009 database based on optimum hybrid features.

Based on all the performance analysis and comparison results, it is concluded that depending on the number of signatures and the selection of appropriate features, the accuracy of classification algorithms differs from one database to another.

7.2 Future Scope

In future, the designed system can be verified by collecting signatures from other standard databases. The best

ITEE, 14 (1), pp. 08-17, FEB2025

Int. j. inf. technol. electr. eng.



ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

extracted features can be selected using other feature selection [13] Tselios, K, Zois, EN, Siores, E, Nassiopoulos, A algorithms to analyze the accuracy of different classifiers for signature verification.

The research work is in progress to utilize the area efficient IIR filter using FPPE for embedding offline signature verification system on FPGA. The designed system can be fused with other biometrics like face and voice to create a multimodal biometric system. The security of the system can be enhanced using block chain technology.

REFERENCES

- P.Shikha and S.Shailja, "Neural Network Based Offline [1] Signature Recognition and Verification System, "Research Journal of Engineering Sciences, 2 (2), pp.11-
- H. Kaur and M. Kumar, Signature identification and [2] verification techniques: state-of-the-art work', Journal of Ambient Intelligence and Humanized Computing, vol. 14, pp. 1027-1045,2023.
- M.O. Oloyede and G.P.Hancke, "Unimodal and [3] multimodal biometric sensing systems: A review," IEEE,(4), pp.7532-7550, 2016.
- L.G.Hafemann et.al, "Offline handwritten signature [4] verification-literature review," (70), pp.163-176, 2017.
- [5] O. A. Hassen, A. A. Abdulhussein, S. M. Darwish, Z. A. Othman, S. Tiun and Y. A. Lofty, 'Towards a secure signature scheme based on multimodal biometric technology: application for IOT Block chain network', Symmetry, vol. 12, pp. 1699,2020.
- V. L. Blankers et.al, "ICDAR 2009 signature verification [6] competition," International Conference on Document Analysis and Recognition, (0),pp.1403–1407, 2009.
- S.T.Panchal and V.V.Yerigeri, "Offline Signature [7] verification based on geometric feature extraction using artificial neural network,"IOSR-JECE, 13(3), pp.53-59,
- Alaei et.al, "An efficient signature verification method [8] based on an interval symbolic representation and a fuzzy similarity measure," IEEE Trans. Inf. Forensics and Secur,, 12, (10), pp.2360-2372, 2017.
- D.Huang and J.Gao, "Online signature verification [9] based on GA-SVM," International Journal of Online and Biomedical Engineering', X, 11, (6), pp. 49-53, 2015.
- D. Yadav and C.Singhal, "Offline signature recognition using PCA NN method and GLDM feature extraction," International journal of advanced research in computer science and software engineering, 5, (9), pp. 258-262,
- [11] Ferrer, MA, Vargas, F, Morales, A& Ordonez, A "Robustness of offline signature verification based on gray level features,"IEEE Trans. Inf. Forensics and Secur, 7, (3), pp.966-977, 2012.
- K. Tselios et.al, "Grid-based feature distributions for offline signature verification," IET Biometrics, 1(1):72,

- &Economou, G ,"Offline signature verification and quality characterization using poset-oriented grid features," Pattern Recognit Lett, Elsevier, 54, pp.162-177, 2016.
- [14] C. Kongtongvattana and T.Phienthrakul, "Signature verification with chain code and geometric features," Proceedings of the 9th International Conference on Machine Learning, (ICMCL),, pp. 342-346, 2017.
- A.V.Bharadwaja, "The analysis of online and offline [15] signature verification techniques to counter forgery," Indian J Sci Technol, 8(20), pp.1-5, 2015.
- D.Pandey and S.Kushwah, "An efficient low level [16] features of CBIR using wavelet, GLDM and SMOSVM method," International Journal of Signal Processing and Pattern Recognition, 10(3), pp.13-22, 2017.
- Pal, S, Alaei, A, Pal, U & Blumenstein, M "Performance of an offline signature verification method based on texture features on a large Indic-script signature dataset,", 12th IAPR Conference on document analysis systems, 2016.
- [18] Sharif, M, Khan, MA, Faisal, M &Yasmin, 'A framework for offline signature verification system: Best Pattern Recognition Letters, features selection', Elsevier, 2018.
- [19] Khokar, S, Zin, AAM, Memon, A, P & Mokhtar, AS, "A new optimal feature selection algorithm for classification of power quality disturbances using discrete wavelet transform and probabilistic neural network," Elsevier measurement, pp.246-259, 2017.
- Mahadi, NA, Mohamed, MA, Mohamad, AI, Kadir, MFA &Mamat, M "A survey of machine learning techniques for behavioral-based biometric user authentication", Recent Advances in Cryptography and Network Security, pp. 44-59, 2018.
- Shyang-Jye Chang and Tai-Rong Wu, 2024, [21] 'Development of a signature verification model based on the small number of samples', in the International journal of Signal, Image and Video Processing.,(18),10,p.285-294.
- Dalal, N & Triggs, B, "Histograms of oriented gradients for human detection", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, (CVPR'05), pp. 1-8, 2005.
- Saraswat, M, Goswami, AK & Tiwar, A, "Object [23] recognition using texture based analysis", International journal of computer science and information technologies, 4, (6), pp. 775-782, 2013.
- Mohanaiah, P, Sathyanarayana, P& Gurukumar, L, "Image [24] texture feature extraction using GLCM approach", International journal of scientific and research publications, ISSN 2250-3153, 3, (5), pp. 1-5, 2013.
- Yekkehkhany, B, Safari, A, Homayouni, S& Hasanlou, M, "A comparison study of different kernel functions for SVM-based classification of multi-temporal polarimetry SAR data", 1st ISPRS International Conference on Geospatial Information Research, Tehran, Iran, pp. 281-285, 2014.



ISSN: - 2306-708X

©2012-24International Journal of Information Technology and Electrical Engineering

- [26] H.Yu and B.M.Wilamowski, "Levenberg-Marquardt Training," Intelligent systems, Auburn University, pp. 12-1-12-16, 2010.
- [27] Chinmay Lokare et.al. 'Offline handwritten signature verification using various Machine Learning Algorithms'', ITM Web of Conferences 40, 03010, ICACC-2021.
- [28] Ibtisam Ghazi Nsaif et.al. 'A Review of Online Signature Recognition system Fusion: Practice and Applications (FPA)', Vol. 18, No. 01. PP. 130-144, 2025
- [29] Wanghui Xiao and Hao Wu, 'Learning features for offline handwritten signature verification using spatial transformer network', Scientific Reports, Vol.15, No: 9453 (2025).
- [30] Jiaxin Lu 1,2, Hengnian Qi et.al, 'Research on Authentic Signature Identification Method Integrating Dynamic and Static Features. Applied Sciences, Vol.12(19), 9904, 2022.

AUTHOR PROFILE



Dr Ramya Rani N received her B.E degree in Electrical and Electronics Engineering from Sri Krishna College of Engineering and Technology, Coimbatore, India in 2008. She received her M.E. degree in Applied Electronics from Kumaraguru College of Technology; Coimbatore, India in 2010. She received her Ph.D degree under the faculty of Information and Communication Engineering from Anna University, Chennai, India in 2020. She has a teaching experience of 9 years. Currently she is working as Assistant Professor in the department of Electronics and Communication Engineering, V.S.B College of Engineering Technical Campus, Coimbatore, India. She has published 18 international journals, 2 books and presented papers in various national and international conferences. She is also an active reviewer for the journal of IET. Her research interest includes VLSI design, image processing and embedded systems.