I.J. Modern Education and Computer Science, **2015, 4, 67-75**
Published Online April 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2015.04.08

An Appraisal of Off-line Signature Verification Techniques

Abdul Salam Shah
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan
Email: shahsalamss@gmail.com

M. N. A. Khan
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan
Email: mnak2010@gmail.com

Asadullah Shah
International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia
Email: asadullah@iium.edu.my

***Abstract*—**Biometrics is being commonly used nowadays for the identification and verification of humans everywhere in the world. In biometrics humans unique characteristics like palm, fingerprints, iris etc. are being used. Pattern Recognition and image processing are the major areas where research on signature verification is carried out. Hand written Signature of an individual is also unique and for identification of humans are being used and accepted specially in the banking and other financial transactions. The hand written signatures due to its importance are at target of fraudulence. In this paper we have surveyed different papers on techniques that are currently used for the identification and verification of Offline signatures.

***Index Terms*—**Biometrics, Offline Signature, Data acquisition, Preprocessing, Forgery.

I. Introduction

The biometrics systems play the most important role in daily routine for the identification of human beings identity. Tomar et al. [1] said the identification of individuals, hand written signature is widely used and accepted mechanism throughout the world, the thorough scrutiny of the signature is important before going to the conclusion about the signee. This variance in genuine signature makes it difficult to differentiate between the genuine and forged signature. The automated Signature verification system may improve the authentication process and can differentiate between the original and forgery signatures. The signature verification and recognition is classified into two major classes: online and offline signature verification system.

A. Types of signatures

There are two main types of signatures that are;

Online signature: In case of online approach the signer sign on the electronic pad in which it becomes easier as compared to offline signature to measure the dynamic features like the speed, writing, stroke applied, direction, pressure applied are extracted which increases the accuracy rate.

Offline signature: In offline approach the dynamic characters of signature cannot be extracted which drops down the accuracy rate, the signature is written on paper and such kind of dynamic information is not available. The dissimilarity in the signature of the same person and greater variance have been observed due to the illness age, time, emotional state, habits or other abnormalities are known as interpersonal variations also the variation among original and forgeries come into the category of inter personal variations.

The forgeries which are related to the signature are mainly classified into the following three types.

B. Types of Forgeries

There are three main types of forgeries which are defined below;

Random forgery: In random Forgeries the signer just knows the name of the victim whose identity he wants to steal. The forger tries the name of victim in different styles to create the random forgery.

Simple forgery: The signer closely observes signature for a moment and then copies it in his own style he does not have any prior experience.

Skilled forgery: In case of skilled forgeries the signer has seen the shape of signature very well and practices on the signature before signing. This type of signature is very difficult to detect and is most challenging to differentiate between the forger and genuine signature.

The hand written signature has also an adequate importance in online banking applications, credit cards, and cheque processing mechanism [2]. For the authentication and validation of passports, biometrics systems can be used; specifically for the signature verification [3]. The Gaussian noise caused by scanning of the document, the difference between the positions of signature in the document, the stamps and other typed

texts which are mixed with the signature that creates some difficulties during the extraction of original signature from the image [4]. There are two main tasks of signature recognition and verification one of them is the correct identification of the owner of signature, and the other is correct classification of signature whether it is a genuine or a forded [5]. The handwritten signatures are the most authentic and realistic use of a person's identification in legal and commercial transactions [6].

The focus of this paper will be on offline signature verification techniques. Further division of this paper will be, in section II contains the literature review of the already published existing techniques of offline signature verification, section III contains the critical analysis table of the all 15 research papers, and finally in section IV the conclusion of paper will be presented.

II. Literature Review

In the field of offline as well as online signature verification and validation lot of research has been done in which many techniques are covered and still many remains to be covered.

Tomar et al., [1] have proposed a model system for the verification of offline signatures, based on the directional feature that are combined with the density features for which extraction process is carried out locally and the aspect ratio is included in the energy density method as global feature. As global feature with the energy density method the aspect ratio was also used for the improvement of the performance of the system. For the training function they have used variable learning rate (triangdx). The authors have compared energy density method with the directional feature method and method proposed by them which is directional feature with energy method, performance parameters of that was training time required, FAR, FRR and accuracy. After performing enough number of observations and experiments they have concluded that, in case if the number of samples of signatures is smaller for the training, the results shown by energy method was best results among the all methods. The training time required in this case is higher than the proposed method, but the accuracy and false acceptance rate was satisfactory, if we consider it as overall the extra time required can be affordable. In case of the huge database which contains large number of both genuine and forged signature for the training process, the energy density method will be good but if we consider the overall performance of the proposed method then it is better than the both two methods. The authors have also observed the variance in results, especially in the FRR, in all cases.

Harika et al. [2] have utilized the two publically available databases for the experiment. The first one is known as MCYT database, which has signatures from 75 genuine signers. For each signer 15 forged signatures and 15 genuine signatures are taken and stored in the database. The second database is known as the GPDS960GraySignature which has signatures collected from 881 signers. The databases contain signatures in the form of checks or invoices. The blending modes that are used during experimentation include linear dodge, color, lighten, linear burn, multiply and darken. For processing of signature only signature strokes are considered, the signature samples has white background. In this paper they implemented the offline signature verification technique presented by Ferrer et al. which uses the technique of histograms of various patterns such as local derivatives, local directional and local binary. During experimentation Different classifiers were used which include SVM, NN. For evaluation of the functionality of the SVM histogram oriented kernels and RBF was used. At the end they had built prototype applications for representing the proof of the concept. Experiments were carried out with both invoices and checks for signature verification automatically.

Odeh et al., [3] have used the GPDS300 signature database which is offered by the Universidad de ias Palmas de Gran Canaria, Spain to those who are willing to do research in field of recognition. The parameters for the signature being original are from 85-100% similarity range. These are based on method of natural signature recognition which says that signatures show some variance on each try from the same person. Furthermore, in case if the similarity percentage is between 75-85% then the measures can be relatively doubtful. In the case where similarity percentage is below than 75% then it is considered as highly doubtful. The experimentation was carried out on an average of 200 signatures and at the end the results was, training accuracy rate: 64% and error rate 36% test accuracy rate 78.8% and error rate 21%. If we conclude the methods and the techniques for the verification and recognition of the signature in this paper they have used MLP neural network. Four features were considered that were skewness, eccentricity orientation and kurtosis. The algorithm used for neural network training was back propagation. At the end they have improved the error rate from 44.9% to 21.1%.

Anjali et al., [4] have proposed two stages model for eliminating or decreasing the background complexity and extracting the original signature form the complex background. The proposed method for removing or reducing the background complexity and extracting the original signature from the complex background has been explained. The blending modes are several like darken, lighten, linear burn or color, linear dodge multiply. In this paper they have used the multiply blend mode, its functioning is to multiply the cheque image with the signature image. Random and simple forgeries are detected here. Here there are 60 signatures which belong to 12 peoples. Each people signed five times. So after training the samples, when these signatures are given for testing it correctly identified the group to which the signature belongs. But when forged signature of the same was given it showed wrong signature. This showed simple forgery. Now if the signature which does not belong to the group was given, it also showed wrong signature. This represents a random forgery.

Deshmukh et al., [5] have proposed a method for verification and recognition of offline signatures based on

neural networks in which the signature has been captured and examined in the form of an image. This model is also writer independent and the pattern recognition process is divided into two major classes of problems which make it possible for the building of robust model, which can be best for the small data sets in which it gives the best result even if the numbers of signatures are small from a signer. There are various successful classifiers for verification of offline signatures, like the Support Vector Machines (SVM) and Hidden Markov Model HMM and they are overall better in the performance than the HMM approaches. The image processing techniques that already exist are of large number for the modification and manipulation of the static images. Like the stroke, color dominant, moment invariant, histogram which can differentiate the signatures of different individuals. The Approach they have proposed consists of step by step processes like the acquisition of the image , image pre-processing, feature extraction, feature as input to the neural network for training using the back propagation algorithm, testing of the signature image and the final on the basis of results classify the signature either it is genuine of forged.

Patil et al. [6] have used the support vector machine which has the fast learning capability and separating the hyper plans in the high dimensional feature spaces. Main goal of this technique is to optimize the simplification bounds. The wavelets are used for the decomposition of signature image after caring out the preprocessing step. The Gaussian Radial Basis Function kernel was used for classification and training. Bounding rectangles were put over the signature; the normalization was done for resizing the signature image with the aspect ratio continued for the original signature. The Resizing of image was carried out with bilinear interpolation method. To represent signature 80 features were used. For faster optimization of the SVM classifier Sequential Minimum Optimization (SMO) technique was used. For the training of SVM classifier, Sequential Minimal Optimization technique is used to carry out the optimization process a bit faster. For the linear kernel the FAR and FRR are 13% and 10% individually. In the case of Radial Basis Function kernel FAR and FRR rates are 15% and 12% respectively. With high level of decomposition of wavelets, proper ranking of features and proper kernel selection for SVM, the results can be improved to some extent.

Pansare et al. [7] have presented a method for geometric feature extraction, preprocessing, training of neural network with extracted features and verification. The effectiveness of the signature verification system depends upon the set of chosen feature vectors for the Hidden Markov Model (HMM). Discrete random transform or Signograph for signature image is calculated at the range of 0 to 360, which are the total pixels of image and their intensity using no overlapping beams per angle for x number of angles. The results have shown AER of 18.4 % for 440 genuine signatures from which 132 was skilled forgeries. The signature database in this paper used is Grupo de Procesadi digital de Senales (DPDS). Once the feature vector of the test signature are applied if the generated value from output layer is +1 then the test signature considered as genuine and if the value generated is -1 then it is declared as forged. This method has 100% correctly identified the signatures into the forged and genuine the network when tested with the different signatures than the signature which were used for training phase, out of 150 genuine signatures and 150 forged signatures the 248 were recognized correctly. This is approximately 83% correct classification in general.

Yilmaz et al., [8] have presented a system based on local histogram features of Offline signature image, for the verification of offline signatures. The first is HOG stands for histogram oriented gradient, and second LBP the local binary patterns. When all classifiers combined the achieved rate of error in test of skilled forgery was 15.41%, and in GPDS- 160 dataset by not including skilled forgeries during training. For making a system which will be strong toward global shape variations, the features were extracted from the signature images local zones. GPDS-300 dataset which is subset of publically available GPDS-960 dataset they have used for the training and testing of system, the data of training and testing were entirely different. Skilled forgeries were used in testing but not considered during training. After analysis the results showed that USVM outperforms GSVM, the USVMs were explicitly trained for individual users and GSVMs were trained for the variations in different dimensions. Global SVM progresses the performance in case if it is used with SVMs in combination. The classifier combination improves overall accuracy. In GSVM use of more references means more data for training and learning to differentiate genuine and forgery signature. The HOG feature which was acquired by polar coordinates beats the other sort of features by USVM with 19.58% EER. The LDP Grid feature results were 19.84% EER. Their results with classifier combination with 12 reference signatures were enhanced as compared to the systems that do not use skilled forgeries for the training. The results of the system they have proposed were lower as compared to the systems those use skilled forgeries for testing, on the basis of local histogram representations automatic signature verification system was proposed.

Darmola et al. [9] have presented an offline signature recognition system by using Hidden Markov Model and Discrete Cosine Transform (DCT). The signatures were divided vertically in to the segments at center of gravity, this division was carried out with the help of pixels reference positions. The results of this experimentation showed that 99.2% correct signature recognition rate is possible. The result of this was better as compared to the systems based on HMM and statistical classifiers. Performance of this system was evaluated according to the False Acceptance Rate (FAR) and False Rejection Rate (FRR). The accuracy of recognition depends upon the ability of reduction of intra variation within signature of the same person and variations within signatures of different persons. This also depends upon the techniques and extracted features that are used for training and

signature classification. The combination of DCT signature features and HMM are combined to develop model framework and signature classification algorithm.

The signature were collected from 250 students at Covenant University Ota, Nigeria, each signer added 7 signature samples into database. Here the features were extracted with DCT at sub image level. DCT transform spatial information of the signature cells into the frequency information in the form of DCT Hidden Markov Model (HMM) which is probabilistic pattern matching technique that has ability of abortion of variability and similarity between signature samples. Hidden Markov Models (HMM) represent signatures as sequence of states. According to the associated probability observation vectors can be generated. Transition probabilities are the transitions between states that are governed by set of probabilities. The probabilities of HMM are then trained with the observation vector which was extracted from samples of signature data. The signature recognition is based on probability that the signature was generated by HMM. Each user signature is demonstrated by guessing the parameters for HMM for a given set of observations. For the training of HMM five signatures from each user were used. For the observation vector set of 16 extracted values from each block were used. The parameters were chosen on the basis of maximum likelihood criterion that maximized the likelihood of observation data. The maximization was performed by the Baum- welch algorithm.

Kanawade et al. [10] have presented a grid base feature extraction of offline signature verification method. The system at initial level was trained with the signature of individuals whose signatures are going to be authenticated by the system. The mean signature will act as source signature for the comparison and verification against the test signature. In this paper they have used the signatures that were collected from internet. This database contains signatures from individuals including the genuine and forgeries. For the processing of signature in this system their image format should be digital. Forgeries were produced by practicing on image of the genuine signatures. Preprocessing was carried out for the improvement of signature image which makes them usable for the feature extraction unit. The scanned images were transformed to black and white images where white is represented by 1 and black by 0. In that way the signature parts were represented with 0 and blank background with 1 that makes coding easier. To make feature extraction easier the gray scale image was converted into binary image. The conversion was carried out with Matlab inbuilt inversion function (~). After applying this function the signature parts were coded by 1 and blank spaces with 0. The additional background was removed. The bounding box was found out, after eliminating blank area from the sides of images. Now the resultant images contain only signature part. Rectangles in signature were constructed that were encompassing the signature. That reduced the area of signature to be used for further processing and saves time. In segmentation the signature contents were extracted for processing further. Thinning was carried out for elimination of the difference in thickness of signatures due to the pen which make it one pixel thick. Two features were used by them for signature recognition and verification. Function Features were velocity, pressure, position. Online signature verification techniques use the function features. The local and global parameters are the subcategories of Parameter features. Wavelet transforms, Fourier transform are global parameters. Pixel oriented and component oriented are the local features. Contour based slant based and geometric based features comes into component oriented features, grid based, intensity based are the sub categories of pixel oriented features. Here they have used grid based feature extraction. The CMS was calculated and in condition where CMS was greater than or equal to 60 then RMS was calculated. The threshold they have set was 65 to 100 for detection of genuine or forged signatures.

Abbas et al. [11] have proposed a system for managing SVM classifier conflicts. This system based on the decision combination, it consists of three different modules i.e. Ridgelet Transform SVM, Radon Transform SVM and PCR5 combination rule that base on generalization belief function of DezertSnarabdache theory. The SVM outputs are merged by this framework and use the technique of estimation. This technique is based of appriou dissonant model for computing belief assignment. For the decision making likelihood ratio was used. CEDAR database was used for the experimentation for the acceptance and rejection of signatures. The proposed system has improved accuracy of verification as compared to the individual SVM classifiers. The offline signature verification methods are less robust as compared to the online signature systems. At the time of designing of system very few characteristics and information about the skilled forger and about forgeries can be obtained. After the deployment of system many unpredicted skills of forgeries can seem at any instance. The most of methods are developed for the feature generation module. For the enhancement in the performance of the Offline signature verification system and ensuring security they have proposed a combinational model based on the individual systems Dezertsmarandache theory (DMST) for management of conflicts between two vector machine classifiers. In this paper they have associated radon based features and Rigelet transforms for every individual system. Using decision rule the output of SVM classifiers were combined DSMT and used for management significantly conflicts generated from individual systems. For the signature verification they took a proposition constraint that $\theta gen \cap \theta imp = \emptyset$ to differentiate between the genuine and forger classes. The main task of combination module which is proposed was the management of conflicts that are generated between two SVM classifiers every signature through the PCR5 combination algorithm. The verification error of both the PCR5 combination model and SVM classifiers was calculated. In Radon transform based offline signature verification system the error of 7.72% to value of threshold t=1.11 and in the Ridgelet

Transform based system results value of threshold t=0.991. The proposer model has improved the error rate of verification by 2.27% for threshold t=0.986. This system showed best results even in the even the offline signature verification provided conflicting outputs.

Ferrer et al. [12] different techniques have been presented on pseudo dynamic features for automation of signature verification. Few of them have utilized gray level values of signature stroke of pixels. The rotation invariant uniform binary pattern gave best results, plus LBP and gray level co-occurrence matrices (GLCM) statistical measures with MCYT and GPDS corpuses for offline signatures. The corpuses that was considered for different studies contains the signatures on white background, but with the complex background of the checks and invoices the variance has been noticed in the gray level distribution of signature image. The measurement of robustness of gray level features that was distorted by the complexity of background was the aim and this paper and further on the basis of that analysis proposes more robust and stable features. For blending of checks and invoices with complex background GPDS and MCYT were used. The blending the most of models functions have used multiplication. The training with genuine signatures was carried out, the signature background was white and these are then tested with the signatures which were combination of genuine and forgeries and they were with different backgrounds. The proposed system based on histogram of local binary, local derivative and local directional patterns for texture measure. The parameters evaluation was carried out with SVM and nearest neighbor. Histogram oriented kernel GHI and classical RBF kernels were used for the evaluation of SVM. Local derivative patterns improve kernel performance and the results as compared to the previous results in different papers. The SVM proved more robust in conflict of gray level distortion in the signatures with difficult background of checks. This configuration was checked in various conditions: by some changes in the number training signature, multiple signing sessions, different ink database, increase in signers and at score level by combining different features. The results also provided when the segmentation of the signature from check was carried out. Among the all cases LDerivP parameters gave best results.

Adke et al. [13] the biometrics has placed at vital position by society due to the higher need of security. Handwritten signatures are from one such biometric behavioral characteristic which is widely accepted attribute for the identification. The major hurdle in the application of signature verification is the forging of signatures. For the mitigation of such forgery the enhancements in the design of classifiers have been used for signature recognition. The research in this area was initiated by developing Artificial Neural Network (ANN) known as Siamese. The combination of ANN with segmentation and spectral analysis was introduced further in addition to this method which is based on moment invariant, support vector machine and Hidden Markov Model was developed to cater the same. The multilayer perceptron MLPs neural network was used by them in this proposed work. The structure of this depend upon the multilayer feed forward, all nodes of one layer are connected with the nodes of second layer bus these are not connected with the nodes of previous layer after that some modification was carried out to get functioning of the back propagation neural network with the help of BP algorithm. Main purpose of this works was determination of how precisely the novel features minimize the error that are prevailed in the existing signature systems. The detailed analysis has shown that the performances of signature verification systems depend upon the classifiers that are utilized and feature that are extracted for the comparison. With few changes desirable classifiers were introduced but the features which were selected for test gave simple results in the all previous research contributors and 44% error rate was reported. After few years the signature verification systems based on ANN as classifies and features as kurtosis, skewness, orientation and eccentricity reported 21% error rate. There is further improvement needed in these terms of error rate and accuracy. Keeping in view the above the authors have proposed a model which focuses on observed vital features aspect and introduces new features viz. 60 points feature and weight * depth value. This is basically further extension of the previous work that has been done with ANN and back propagation algorithm as classifier. The proposed work was tested on the benchmarks of GPDS 300 signatures database. These results have indicated that the performance has been enhanced in terms of 88% in accuracy and error rate was reduced by 9%. This work can be further extended by making some changes into existing classifier by taking same 60 points features. It can be predicted by testing different classifiers with the same 60 points feature for further improvement of performance in the offline signature verification and recognition system.

Prashanth et al. [14] have proposed Angular features OSVAF based offline signature verification system. The images after scanning are preprocessed and the signature part from the unnecessary background is obtained. In first stage the center of signature image was calculated by count of number of pixels in each block and this was used for the division of each signature into 128 blocks. After that the angular features were determined in each block for the generation of 128 angular features. In second stage 40 block of each signature was created from the corner of signature for generation of 40 angular features. During the experiment total 168 angular features were considered from the first and second phase for the verification of signature. Then Variance between test signature angular features and genuine signature was calculated and later they are compared with the threshold for the authentication of the signature. After observation it reveals that the system performance as FAR, FRR and EER wise was better than the existing algorithms. The OSVAF algorithm which is based on the angular features has shown more efficiency and gave better results as compared to the existing techniques. The threshold was if the number of differences is greater than the threshold

counted as if the number is greater than 133 out of 168 then signature was considered as genuine. The better result can be achieved if the preprocessing is carried out in transform domain. The proper use of SVM achieves further reduced error rates.

Zois, et al., [15] have presented different approach of verification and recognition of offline signature. For the representation of the signature curvature features were used; subset of line, convex and concave. Two constraints were applied for feature extraction and to model the transitional probabilities of signature pixels. The signature trace segmentation was enabled through window that lies at center of the mass of signature image which was already thinned. The multidimensional feature vector is created by dividing the image into portions for the spatial details of signature image. Hard margin support vector machine (SVM) based protocol was used for classification. Two databases were used in this method, the first taken from previous literature and second generated by the authors. To achieve comparable results, already published method for feature extraction was used, with same classification protocol. After basic evaluation of both corpuses it has shown good verification average error results. If we talk about the results of both corpuses of the method they have proposed, there was 0.5% probability of false alarm (FAR), which was very low. The FAR probability of 0.01% was achieved. For the FRR measure they have observed that corresponding probability of error decrease with the increase of genuine signature samples in the classifier. FAR error increases with augmentation of genuine training sample set. This is due to tradeoff between FAR and FRR. The model absorbs the interpersonal variability of adding further original samples; it lets the FAR to increase by embracing more forged samples. This method has given better results than the previous schemes of FAR, FRR and AvE. This assumption is a little bit valid for the CORPUS1 database. The CORPUS1 has small number of samples than CORPUS2. In the first three cases of CORPUS1 average error rate was pretty large. The local line feature that was extracted from different parts of the test image was summed up; these features were the curvature and orientation. The counter was updated for each pixel of the signature trace on every component found, by marking the path that was involved in feature set. For the evaluation of proposed method they have compared with the already published system for the strengths of method. For every signer a SVM classifier which was dedicated has been employed in the first stage of verification. Iqbal et al. [16,17] proposed performance metrics for software design and software project management. Process improvement methodologies are elaborated in [18,19] and Khan et al. [20] carried out quality assurance assessment. Amir et al. [21] discussed agile software development processes. Khan et al. [22] and Khan et al. [23] analyzed issues pertaining to database query optimization and requirement engineering processes respectively. Umar and Khan [24,25] analyzed non-functional requirements for software maintainability. Khan et al. [26,27] proposed a machine learning approaches for post-event timeline reconstruction. Khan [28] suggests that Bayesian techniques are more promising than other conventional machine learning techniques for timeline reconstruction. Rafique and Khan [29] explored various methods, practices and tools being used for static and live digital forensics. In [30], Bashir and Khan discuss triaging methodologies being used for live digital forensic analysis. References [31-47] reviewed different techniques in different domains and reported their critical evaluations along with a workable framework where necessary.

III. Critical Evaluation

Table 1. Evaluation of Offline Signature Verification Techniques.

Author (s)	Technique	Focus area	Strengths	Limitations
[1]	Directional Feature and Energy Density. Neural Network as Classifier.	Skilled Forgeries	Directional feature with energy method gives Improved results as compared to the previous two methods.	Do not give accurate results in case of large number of signature database.
[2]	Support Vector Machine (SVM). RB, histogram oriented kernels.	Gray Level Features	The SVM with kernel has proved more robustness against gray level distortion mixed with signature images with bank checks.	Signature's gray level distribution changes when the background is complex i.e. checks and invoices.
[3]	Multi-Layer Perceptron's Neural Network. Back-propagation algorithm used for training.	Eccentricity, Skewness, Kurtosis, Orientation.	A 21.2% error stated by this approach, a great progress over previous methods that reported error rate of 44.9% Multilayer perceptron's have capability to solve extremely complex problems accurately.	Neural Network finds out to solve problem by itself, which makes its operations unpredictable.
[4]	Gray level Distribution in Signature Strokes and Neural Network as Classifier.	Reducing the Background Complexity	Gradient has reduced the error rate. The neural network identified the group to which the signature belongs accurately.	This system cannot differentiate properly between simple forgery and random forgery. Not suitable for the small number dataset.

[5]	Artificial Neural Network (ANN)	Strokes, moment invariants, GLCM, color dominant, histogram	Euclidian Distance was used which gave success rate of 84.1%. Their ability to learn by example makes neural nets very flexible and powerful	The neural networks learn according case to case and they do not follow the instructions that are provided by the authors.
[6]	Discrete Daubechies (db4) Wavelet Transform and Support Vector Machine (SVM)	Wavelet features	Wavelet transform is suitable for applications where information offered is hardly denoted by functions.	High level wavelet decomposition of image and ranking of features can improve results. Suitable kernel selection and setting the kernel parameters is success of this method.
[7]	Image prepossessing, geometric feature extraction.	Direction, surface area, length skew and centroid features.	Stochastic models having capacity of absorbing variance in patterns and their similarities.	It gives poor performance on signatures which was not included in training.
[8]	Global and user dependent SVMs for classification.	Rectangular or polar grids, where HOG and LBP features are calculated.	Combination of classifiers, showed improved overall performance of verification. Skilled forgeries are not required to be enrolled by users.	Training not carried out with skilled forgeries.
[9]	Discrete cosine Transform (DCT) and Hidden Markov Model (HMM).	Sequence Analysis in Signature.	HMM implementation is simple. To model Signature HMM is used. HMM have capacity of absorbing the variability among patterns and their resemblances.	HMM have limitations; defining best algorithm for modeling is difficult.
[10]	Grid based Feature Extraction.	Gray scale and binary image.	Rectangle encompassing the signature reduces area for processing and saves time. The logical comparisons become easier with the conversion of signature parts into binary 0 and 1.	For generation of vector matrix the points are recognized diagonally to analyze more points for getting accurate results than simple grid.
[11]	Dezert-Smarandache theory (DSmT). Support Vector Machine (SVM) classifier.	Features based on Radon and ridge let transforms	The proposed combination framework with PCR5 rule yields the best verification accuracy even with the conflicting outputs by individual offline classifications.	The major limitation of the SVM lies in selection of the kernel and also the limitation of speed and size for training and testing.
[12]	Gray level features and SVM classifier.	To measure robustness of gray level features of distorted and complex background image.	It is clear from results that Local binary patterns or local derivative and directional patterns are more robust than rotation invariant uniform LBP or GLCM features to the gray level distortion.	The LBPs variations are still sensitive to random noise and non-monotonic illumination variations.
[13]	Multilayer Perceptron MLPs Neural Network.	Considered 4 features: eccentricity, kurtosis, orientation and skewness.	The performance of system enhanced by 88% accuracy and error rate was reduced by 9%.	Neural networks give poor results where training data is small. By changing classifiers, results can be further improved.
[14]	Off-line Signature Verification based on Angular Features (OSVAF)	Angular Features of test signature.	The OSVAF is an efficient algorithm than the other techniques and it gives best results. This algorithm is based on angular features.	Transform domain preprocessing can improve the results further. The errors can be reduced further with the use of SVM.
[15]	Two step Transitional Features	Evaluation of the random forgeries	Boolean masks are used for features extraction from binary images that makes system feasible and hardware implementation faster.	Skilled forgeries, texture and chain based features were not considered.

VI. Conclusion And Future Work

This paper has focused on the offline signatures and the techniques that are used for the verification and validation of signature for the classification of them into the genuine or forgery. The verification of signature is carried out on the basis of the features of signature that are extracted using different static image processing techniques. As this paper contains the review of literature in continuation to this the next objective will be to propose some new model that will reduce the FAR and FRR.

References

[1] M. Tomar, and P. Singh, "A directional feature with energy based offline signature verification network," *International Journal on Soft Computing*, vol.2, pp. 48–57, February 2011, "doi: 10.5121/ijsc.2011.2105".

[2] K. Harika, and T.C.S. Ready, "A tool for robust offline signature verification," *International journal of advanced research in computer and communication engineering*, vol.2, pp. 3417–3420, September 2013.

[3] S. Odeh, and M. Khalil, "Apply multi-layer perceptron neural network for off-line signature verification and recognition," *IJCSI International Journal of Computer Science Issues*, vol.8, pp. 261–266, November 2011.

[4] R. Anjali, and M.R. Mathew, "An efficient approach to offline signature verification based on neural network," *IJREAT International Journal of Research in Engineering & Advanced Technology*, vol.1, pp. 1–5, June-July 2013.

[5] V.M. Deshmukh, and S.A. Murab, "Signature recognition & verification using ANN," *International Journal of Innovative Technology and Exploring Engineering*, vol.1, pp. 6–8, November 2012.

[6] G.P. Patil, and R.S.Hegadi, "Offline handwritten signatures classification using wavelets and support vector machines," *International Journal of Engineering Science and Innovative Technology*, vol.2, pp. 573–579, July 2013.

[7] A. Pansare, and S.Bhatia, "Handwritten signature verification using neural network," *International Journal of Applied Information Systems*, vol.1, pp. 44–49, January 2012.

[8] M.B.Yilmaz, B. Yanikoglu, C. Tirkaz, and A. Kholmatov, "Offline signature verification using classifier combination of HOG and LBP features," *IEEE, In Biometrics (IJCB)*, pp. 1–7, 2011 [*2011 International Joint Conference*, p.1–7, 2011].

[9] D.S.A. Daramola, and P.T.S. Ibiyemi, "Offline signature recognition using hidden markov model (HMM)," *International Journal of Computer Applications*, vol.10, pp. 17–22, November 2010.

[10] M.V. Kanawade, and S.S. Katariya,"Offline signature verification and recognition," *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development*, vol.3, pp. 107–114, August 2013.

[11] N. Abbas, and Chibani, "SVM-DSmT combination for off-line signature verification," *International Conference on Computer, Information and Telecommunication Systems*, pp.45–56, May 2012.

[12] M.A. Ferrer, J.F. Vargas, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features," *IEEE Transactions on Information Forensics and Security*, vol.7, pp.966–977, June 2012.

[13] S. Adke, and P.A.P. Khekar, "An enhanced artificial neural network based offline signature verification and recognition system," *International Journal of Engineering Research & Technology*, vol.2, pp. 175–178, December 2013.

[14] C.R. Prashanth, and K.B. Raja, "Off-line signature verification based on angular features," *International Journal of Modeling and Optimization*, vol.2, pp. 477–481, August 2012.

[15] E.N.Zois, A.Nassiopoulos, K.Tselios, E.Siores, and G.Economou, "Off-line signature verification using two step transitional features," MVA2011 Conference on Machine Vision Applications, pp. 295–298, June 2011.

[16] Iqbal S., Khalid M., Khan, M N A. A Distinctive Suite of Performance Metrics for Software Design. International Journal of Software Engineering & Its Applications, 7(5),(2013).

[17] Iqbal S., Khan M.N.A., Yet another Set of Requirement Metrics for Software Projects. International Journal of Software Engineering & Its Applications, 6(1),(2012).

[18] Faizan M., Ulhaq S., Khan M N A., Defect Prevention and Process Improvement Methodology for Outsourced Software Projects. Middle-East Journal of Scientific Research, 19(5), 674-682,(2014).

[19] Faizan M., Khan M NA., Ulhaq S., Contemporary Trends in Defect Prevention: A Survey Report. International Journal of Modern Education & Computer Science, 4(3),(2012).

[20] Khan K., Khan A., Aamir M., Khan M N A., Quality Assurance Assessment in Global Software Development. World Applied Sciences Journal, 24(11),(2013).

[21] Amir M., Khan K., Khan A., Khan M N A., An Appraisal of Agile Software Development Process. International Journal of Advanced Science & Technology, 58,(2013).

[22] Khan, M., & Khan, M. N. A. Exploring Query Optimization Techniques in Relational Databases. International Journal of Database Theory & Application, 6(3). (2013).

[23] Khan, MNA., Khalid M., ulHaq S., Review of Requirements Management Issues in Software Development. International Journal of Modern Education & Computer Science, 5(1),(2013).

[24] Umar M., Khan, M N A., A Framework to Separate Non-Functional Requirements for System Maintainability. Kuwait Journal of Science & Engineering, 39(1 B), 211-231,(2012).

[25] Umar M., Khan, M. N. A, Analyzing Non-Functional Requirements (NFRs) for software development. In IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), 2011 pp. 675-678), (2011).

[26] Khan, M. N. A., Chatwin, C. R., & Young, R. C. (2007). A framework for post-event timeline reconstruction using neural networks. digital investigation, 4(3), 146-157.

[27] Khan, M. N. A., Chatwin, C. R., & Young, R. C. (2007). Extracting Evidence from Filesystem Activity using Bayesian Networks. International journal of Forensic computer science, 1, 50-63.

[28] Khan, M. N. A. (2012). Performance analysis of Bayesian networks and neural networks in classification of file system activities. Computers & Security, 31(4), 391-401.

[29] Rafique, M., & Khan, M. N. A. (2013). Exploring Static and Live Digital Forensics: Methods, Practices and Tools. International Journal of Scientific & Engineering Research 4(10): 1048-1056.

[30] Bashir, M. S., & Khan, M. N. A. (2013). Triage in Live Digital Forensic Analysis. International journal of Forensic Computer Science 1, 35-44.

[31] Sarwar, A., & Khan, M. N. (2013). A Review of Trust Aspects in Cloud Computing Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2(2), 116-122.

[32] Gondal, A. H., & Khan, M. N. A. (2013). A review of fully automated techniques for brain tumor detection from MR images. International Journal of Modern Education and Computer Science (IJMECS), 5(2), 55.

[33] Zia, A., & Khan, M. N. A. (2012). Identifying key challenges in performance issues in cloud computing. International Journal of Modern Education and Computer Science (IJMECS), 4(10), 59.

[34] Ur Rehman, K., & Khan, M. N. A. (2013). The Foremost Guidelines for Achieving Higher Ranking in Search Results through Search Engine Optimization. International Journal of Advanced Science and Technology, 52, 101-110.

[35] Khan, M., & Khan, M. N. A. (2013). Exploring query optimization techniques in relational databases. International Journal of Database Theory & Application,6(3).

[36] Shehzad, R., KHAN, M. N., & Naeem, M. (2013). Integrating knowledge management with business intelligence processes for enhanced organizational learning. International Journal of Software Engineering and Its Applications, 7(2), 83-91.

[37] Ul Haq, S., Raza, M., Zia, A., & Khan, M. N. A. (2011). Issues in global software development: A critical review.

Journal of Software Engineering and Applications, 4(10), 590.
[38] Zia, A., & Khan, M. N. A. (2013). A Scheme to Reduce Response Time in Cloud Computing Environment. International Journal of Modern Education and Computer Science (IJMECS), 5(6), 56.
[39] Khan, M., & Tariq, M. (2011). The Context of Global Software Development: Challenges, Best Practices and Benefits. Information Management & Business Review, 3(4).
[40] Shahzad, A., Hussain, M., & Khan, M. N. A. (2013). Protecting from Zero-Day Malware Attacks. Middle-East Journal of Scientific Research, 17(4), 455-464.
[41] Khan, A. A., & Khan, M. (2011). Internet content regulation framework. International Journal of U-& E-Service, Science & Technology, 4(3).
[42] Kaleem Ullah, K. U., & MNA Khan, M. K. (2014). Security and Privacy Issues in Cloud Computing Environment: A Survey Paper. International Journal of Grid and Distributed Computing, 7(2), 89-98.
[43] Abbasi, A. A., Khan, M. N. A., & Khan, S. A. (2013). A Critical Survey of Iris Based Recognition Systems. Middle-East Journal of Scientific Research, 15(5), 663-668.
[44] Khan, M. N. A., Qureshi, S. A., & Riaz, N. (2013). Gender classification with decision trees. Int. J. Signal Process. Image Process. Patt. Recog, 6, 165-176.
[45] Ali, S. S., & Khan, M. N. A. (2013). ICT Infrastructure Framework for Microfinance Institutions and Banks in Pakistan: An Optimized Approach.International Journal of Online Marketing (IJOM), 3(2), 75-86.
[46] Mahmood, A., Ibrahim, M., & Khan, M. N. A. (2013). Service Composition in the Context of Service Oriented Architecture. Middle East Journal of Scientific Research, 15(11).
[47] Masood, M. A., & Khan, M. N. A. (2015). Clustering Techniques in Bioinformatics. I.J. Modern Education and Computer Science, 2015, 1, 38-46.

Authors' Profiles

Abdul Salam Shah is currently doing postgraduate degree in computer science from SZABIST Islamabad Pakistan. He did his BS degree in computer science from Isra University Hyderabad, Sindh Pakistan in 2012. In addition to his degree he has competed short courses and diploma certificates in databases, cybercrime, networking and software engineering.

He has published articles in various journals of high repute. He is a young professional and he started his carrier in the Ministry of Planning, Development and Reforms, Islamabad Pakistan. His research area includes Machine Learning, Artificial Intelligence, Digital Image Processing and Data Mining.

Mr. Shah has contributed in a book titled "Research Methodologies; an Islamic perspectives," *International Islamic University Malaysia*, in press.

M. N. A. Khan obtained D.Phil. degree in Computer System Engineering from the University of Suusex, England. His research interests are in the fields of software engineering, cloud computing, cyber administration, digital forensic analysis and machine learning techniques.

Dr. Asadullah Shah is working as Professor at the Kulliyyah of ICT, International Islamic University Malaysia (IIUM) before joining IIUM, he worked as Head of Telecommunication Engineering & Management department, IoBM Karachi Sindh, Dean Faculty of Computer and Management Sciences, Isra University Hyderabad Sindh and Head of Telecommunication Engineering and IT, Sukkur IBA, Sindh-Pakistan.

He did his PhD from university of Surrey UK, in 1998, with specialization in Multimedia Communication. He started his academic carrier from University of Sindh Jamshoro, Pakistan in 1986 as a lecturer.

He has published 150 research articles in highly reputable international and national journal in the field of computers, communication and IT. Also he has published 12 books in his 28 years of academic carrier. Currently he is supervising great number of postgraduate students, working in multiple disciplines, specially, animation, social media and image processing in the Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

