Proceedings of
INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND ENERGY SYSTEMS (ICCCES-16)
In Association with IET, UK & Sponsored by TEQIP-II
29th -30th, Jan. 2016

Paper ID:CSEIT32

ENHANCED SCHEME FOR HANDWRITTEN OFFLINE SIGNATURE VERIFICATION

Mrs. Rutuja M. Shinde
Nagraj V. Dharwadkar
Department of Computer Science and Engineering RIT, Sakharale, Islampur (Maharashtra), India

Abstract— Handwritten Signature Verification is a broad area. It has been broadly researched in the last decades but there is an open research problem. There are some possibilities to improve the results. To achieve better results we propose a new handwritten offline signature system. The non-repetitive nature of variation of the signature, because of age and illness this is the limitation of existing system. To overcome this limitation this new system is design. Signature having own psychology or behavior characteristics using that we will propose system to find nature and current psychology of signature person in offline. Different features are extracted from offline signature for comparison. One-class SVM (Support Vector Machine) classifier is used for classification of signature. Signature is genuine or forged one to classify that OCSVM (One-Class Support Vector Machine) used.

Keywords— Offline signature verification, One class Support Vector Machine, Biometric Authentication, False Acceptance Rate(FAR), False Rejection Rate(FRR)

I. INTRODUCTION

Person identification is differentiated by Signature. Now days an increasing number of financial transactions, are being authorized via signatures. Authentication of an individual or a document, signature is used as one of the biometric hallmarks.

In authentication of official documents like bank checks, credit card transactions, certificates, contracts and bonds signature popularly used. The aim of an automatic signature verification system is to validate the individual's identity which is signature analysis of person [1]. There are mainly two types of signature verification systems: offline and online.

Special devices used by the users in online systems are special pens and tablets to acquire signature trajectory dynamics such as pressure, velocity etc. In offline signature verification systems employ digitized signature images through scanner for authentication. Offline Signature images gives only static information which produces less informative signals and therefore, pattern recognition is harder task. The verification of offline signature contains following steps [3]:

(a) Data Acquisition: The data acquisition can be done in two way- in first way signature database is available on internet we can take that database. In second way scanning is done to convert signature image into digital image.

(b) Image Pre-Processing: Numerous operations are perform on signature image in image pre-processing such as getting gray image from color image, noise removing, thresholding, thinning, detecting boundary and image cropping. The binarization consist of converting a color image into black and white image which is represented by "1" and "0" where "1" stands for pixel of signature and "0" stands for pixel of background.

(c) Feature Extraction: In this stage, extraction of features from signature image is performed and for this purpose different algorithms are used. Classification of features can be done as global, grid and mask features. Wavelet coefficient and Fourier coefficients is text provided by global features. Information regarding direction of the signature lines is represented by the mask features. Information about appearance of the signature is given by grid features. Set of features selection is difficult in signature verification systems because the features used must be suitable for the application.

The paper is organized as follows: we outline some relevant previous work done in Section II. In section III we describe our proposed Offline signature verification in detail. The results and analysis are presented in section IV and finally, section V offers concluding remarks and future work.

II. RELATED WORK

There are different classifiers are used to classify signature in forgery or genuine one. These classifiers such as naives' base classifier, support vector machine, neural network etc. Signature is for authentication of person. In authentication of official documents like bank checks, credit card transactions, certificates, contracts and bonds signature popularly used.

In [1], Rajesh Kumar et al. presented a set of signature features which is based on surroundedness property for offline signature verification. Author proposed feature set that describes both shape and texture property of the signature. Two classifiers are used multilayer perceptron (MLP) and support vector machine to examine the efficacy of the proposed features and this is tested on two publicly available database namely, GPDS300 corpus and CEDAR signature database. As compare to the state-of-the-art methodologies, it has been seen that the proposed system is superior either in terms of accuracy or the time complexity or both.

In [2], George S. Eskander et al. introduced writer-independent systems for this signature templates are needed for verification. Standard signature verification systems are writer dependent, in that specific classifier is designed for each individual. It is inconvenient to ask a user to provide

enough number of signature samples to design his WD classifier. To overcome this WI systems are introduced. Author proposed a hybrid WD-WI system.

Simulation results on two real-world offline signature databases confirm the feasibility and robustness of the proposed approach. The final user-specific WD verification mode showed enhanced accuracy with decreased computational complexity. The produced WD classifiers are more secure than the baseline WI classifiers, eliminating the need to store user templates for verification.

In [3], Kruthi. C et al. developed support vector machine for identity verification of offline signature based on feature values in the database. A set of signature samples are collected from individuals and these signature samples are scanned in a gray scale scanner. These scanned signature images are then subjected to a number of image enhancement operations like binarization, complementation, filtering, thinning and edge detection. The values from the database are fed to the support vector machine which draws a hyper plane. On the basis of signature feature value, signature is classified into original or forged. After pre-processing features such as aspect ratio, centroid, number of loops, area and slant angle are extracted from signatures. These feature set are separately passed through the support vector machine developed using kernel perceptron, which are tested against both linear and polynomial kernel.

In [4], Yasmine Guerbai et al. produced a Handwritten Signature Verification System (HSVS). The main problem for designing HSVS is the limited number of writers and genuine signatures. Authors proposed use of One-Class Support Vector Machine (OC-SVM) based on writer-independent parameters, which takes only genuine signatures into consideration and for designing the HSVS forgery signatures are lack. The main advantage of the proposed HSVS is that it allows designing the HSVS using few writers and signatures. It allows also defining an only optimal threshold from genuine and fictitious signatures derived from the combination of
distance used into the OC-SVM kernel, which should be carefully adjusted. When a new writer is presented to the system, the same parameters of the OC-SVM are used without finding the optimal threshold. This paper gives better performance as compare to the state of the art.

In [5], Bence Kovari et al. proposed a simplified probabilistic model for offline signature verification. In this model, each of the verification steps can be described mathematically. It is individually analyzed and improved. To predict the accuracy of a signature verification system based on just a few a priori known parameters, such as the cardinality and the quality of input samples this model was used. To characterize this class of problem they proposed a framework that provides a quantitative way. Verification of baseline and loop feature properties is done using normality tests, and that could be efficiently similar with a normal distribution. Differentiation between original signature and forgeries can successfully done using local features with this system.

In [6], Srikanta Pal et al. proposed an empirical contribution using a novel method towards the understanding of signature verification involving offline Hindi signatures. An offline verification system involves hindi signatures performance investigated, whose style is distinct from Western scripts. Here, for signature verification gradient feature, Zernike moment features and SVMs were considered. Hindi offline signature dataset offers an effective contribution to the field of non-Western signature verification.

In [7], Luana Batista et al. proposed Hybrid generative-discriminative ensembles of classifiers (EoCs). Author designed an offline signature verification (SV) system from few samples on the basis of classifier selection process which is dynamically performed. Multiple discrete left-to-right Hidden Markov Models (HMMs) are trained by using a different number of states to design the generative stage and code book sizes, which allows for the system learn signatures at different levels of perception. In designing discriminative stage, for each training signature HMM likelihoods are measured, and assembled into feature vectors for classification using a specialized Random Sub space Method. The hybrid generative-discriminative system gives greater performance than other systems.

In [8], Jacques Swanepoel et al. presented a modelling framework as a novel dissimilarity-based signature for writer-independent offline signature verification. Author proposed a framework which utilize algorithm are a Discrete Radon transform and a dynamic time warping in dissimilarity space for the representation of writer-independent signature, and a writer-specific strategy for dissimilarity normalisation. For verification purposes a discriminative classifier utilized, either a discriminant function or a support vector machine. In that
of both linear and non-linear decision boundaries are taken into consideration. This study provides an improved platform that is presented by the authors to show that the novel techniques for writer-independent signature modelling.

When evaluated on Dolfing's data set, a signature database that contains 1530 genuine signatures and 3000 skilled forgeries, the systems presented in this study outperform all previous systems also evaluated on this data set.

In [9][11], authors presented that on a uniform white "non distorting" background signatures are written which is the content of corpuses, and on the complex background like check and invoice the signature is written due to which signature strokes changes in the gray level distribution. Author ensured robustness of gray level features when it is distorted by a complex background and also to propose more stable features. The signature models are trained with genuine signatures on white background and tested with other genuine and forgeries mixed with different backgrounds. Results show that a basic version of local binary patterns (LBP) or local derivative and directional patterns are more robust than rotation invariant uniform LBP or GLCM features to the gray level distortion when using a support vector machine with histogram oriented kernels as a classifier.

In [12], author proposed technique is based on the grid features extraction. For verification, the extracted features of test signature are compared with the already trained features of the reference signature. This technique is suitable for various applications such as bank transactions, passports etc. The threshold used in the proposed technique can be dynamically changed according to the target application. The proposed technique deals with skilled forgeries. From comparative analysis it has been observed that proposed technique gives better FAR and FRR for both databases than existing verification techniques.

III. PROPOSED OFFLINE SIGNATURE VERIFICATION SYSTEM

Now days the human signature of a person is used as an identification of person because we are all know that the each person has distinct signature and every signature has its own physiology or behavioral characteristics. Verification of signature is very important. Offline signature is genuine or forged one this will be recognized by existing system. Rapidly, accurate verification of signature will be done. The non-repetitive nature of variation of the signature, because of age and illness this is the limitation of existing system.

As above mentioned signature having own psychology or behavior characteristics using that we will propose system to find nature and current psychology of signature person in offline. To overcome this we will propose handwritten offline signature verification system for all signatures by extracting features from signature image. This system will improve the performance in terms of accuracy. Therefore it will help to verify signature is genuine or forged one. The proposed system will give better results than existing system. Architecture of proposed work is shown in figure-1. Input for system is a scanned image of signature.

There are 4 steps: Data acquisition, image preprocessing, feature extraction and classification. In training and testing phase this steps are same. Classifiers are trained in training phase and knowledge based database is created for further use. In testing phase, trained classifiers and knowledge base is applied on extracted feature points to verify signature.

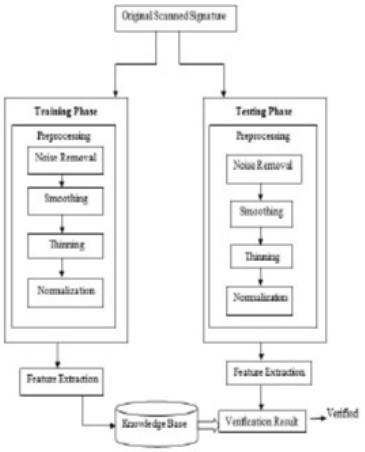

Figure 1: System Architecture

Above architecture shows that scanned offline signature is given as input. After that features are extracted from that signature such as slant angle, height, width, number of black pixels, centroid of the signature, dimension of the signature. In grid features cropped image is divided into 9 rectangular segments i.e. (3*3) blocks. These features are extracted from the signature image.

After this extraction process signature is classify as genuine or forgery by using one class support vector machine. Lastly we got verification result as signature gets verified or not.

IV. EXPERIMENTAL RESULT

This fig.2 is the signature image. This image shows signature we have to do shifting, rotating, scaling and noisy image.

Figure 2: Reference signature

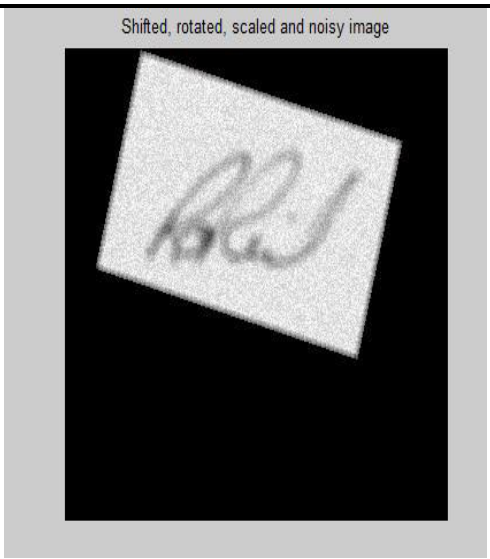

Figure 3: Processing on signature

Above fig. 3 shows that after processing of signature. In that shifting, rotating and scaling is done. After that noisy image is shown.

Figure 4: Converting image into RGB to gray and edge detection

Above fig.4 shows that conversion of RGB into gray scale. Signature converted into binary image. After that edge detection is done.

Figure 5: Select signature from GPDS dataset

In fig.5 shows that open signature from GPDS dataset and opened signature is saved in database. Signature is saved for next process means feature extraction.

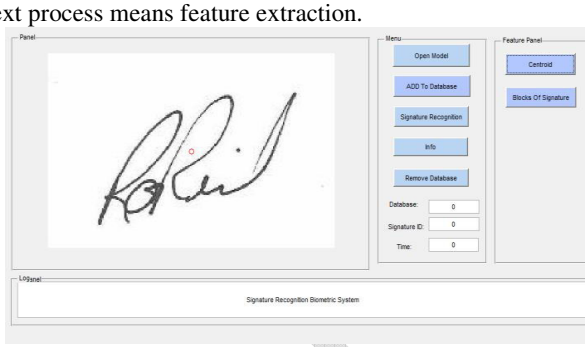

Figure 6: Centroid of selected signature after cropping

Above fig.6 shows centroid of the selected offline signature image. Red point shows that centroid of signature.

Figure 7: Blocks of signature

Above fig.7 shows signature is divided in 9 blocks or segments i.e. (3*3) blocks.

CONCLUSION

In this paper we propose new handwritten offline signature which extracts grid features from the signature. Offline signature verification system gives signature is genuine or forgery one. We did experiment on GPDS dataset. GPDS dataset consist of 4000 signatures. In this dataset skilled as well as forgery signatures are given. Here we are finding centroid of the signature. In future work we do our next part that is remaining in this.

REFERENCES

[5] Kumar Rajesh, J. D. Sharma, Bhabatosh Chanda, "Writer-independent off-line signature verification using surroundedness feature," Elsevier, pp. 301-308, February 2012.

[6] George S. Eskander, Robert Sabourin, Eric Granger, "Hybrid writer independentwriter-dependent offline signature verification system," IET Biom., Vol. 2, Iss. 4,pp. 169-181, June 2013.

[7] Kruthi C., Deepika C. Shet, "Offline signature verification using support vector machine," Signal and Image Processing, 2014 Fifth International Conference on. IEEE, 2014.

[8] Guerbai Yasmine, Youcef Chibani, Bilal Hadjadji, "The effective use of the one-class SVM classifier for handwritten signature verification based on writerindependent parameters," Elsevier, pp. 103-113, August 2014.

[9] Kovari Bence, Hassan Charaf, "A study on the consistency and significance of local features in off-line signature verification," Elsevier, pp. 247-255, November 2012.

[10] Pal Srikanta, Umapada Pal, Michael Blumenstein, "Off-line verification technique for Hindi signatures," IET Biom., Vol. 2, Iss. 4, pp. 182-190, October 2013.

[11] Luana Batista, Eric Granger , Robert Sabourin, "Dynamic selection of generativediscriminative ensembles for off-line signature verification," Elsevier pp. 1326-1340, October 2011.

[12] Swanepoel Jacques, Johannes Coetzer, "A robust dissimilarity representation for writer-independent signature modelling," IET Biom., Vol. 2, Iss. 4, pp. 159-168,May 2013.

[13] Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, "Robustness of offline signature verification based on gray level features," IEEE Transactions On Information Forensics And Security, Vol. 7, No. 3, pp. 966-977, June 2012.

[14] Kumar Manoj, Niladri Puhan, "Off-line signature verification: upper and lower envelope shape analysis using chord moments," IET Biom., Vol. 3, Iss. 4, pp. 347-354, July 2014.

[15] J. Vargas, Jesus Ferrer, C.Travieso, J.Alonso, "Off-line signature verification based on grey level information using texture features," Elseiver, pp. 375-385, July 2010.

[16] Srivastava Swati, Suneeta Agarwal, "Offline signature verification using grid based feature extraction," International Conference on Computer Communication Technology (ICCCT) IEEE, pp. 185- 190, 2011.