© 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

Optimizing Handwritten Signature Verification

[1]Prajapati Pravin,[2]Viral Borisagar
[1]PG scholar,[2]Assistant Professor
[1]Department of Computer Engineering
[1]Government Engineering College, Sector 28, Gandhinagar

***Abstract* – Signature recognition is probably the oldest biometrical identification method, with a high legal acceptance. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. We have worked on the Offline Verification of signatures. In proposed method we have tried to reduce requirement of large number of genuine sample for training by using more common feature of signer like signature area ,signature height to width ratio, distribution of pixel, lbp, optical flow . I have use support vector machine for classification of signature into genuine or forged.**

***IndexTerms* – off line signature verification , SVM.**

I. INTRODUCTION

From long time, signature is widely used as identity metric. On document signature is give assurance of originality of document. In the history, the royal documentation need stamp on it to ensure originality of document. In Visigothic Legal system, the confirmation of document is done by witnesses who have touched it and signed it. It is best branch of Germanic law. Many time private document need to be conformed by royal document. [6]..

Biometrics is the general term to refer to the automatic use of physiological characteristics (e.g., face, iris, fingerprint) or behavioral traits (e.g., signature, key-stroke dynamics) for authenticating the identity of an individual [7]. Among biometric traits, a handwritten signature is one of the most interesting since people are familiar with the use of signatures in their daily life. In addition, In many administrative and financial institutions a signature is generally used to legally verify an personal identity [8].

We need a better verification system, that automatically inspect authenticity of the handwritten signature with the help of some method that will efficiently find out forgery. [9].There are two approaches for signature verification based on the acquisition of the data: On-line and Off-line. If electronic instrument like tablet or digital pen is used for obtaining signature data than method is known as online signature verification. In online approach data is obtain during writing time so there is dynamic information like writing speed, pressure applied and number of strokes is available. If images of signature is used to obtain signature data than method is known as off line signature verification. Here signature written on paper is converted into images with the help of a camera or a scanner. In off line approach, the dynamic information is missing. Processing of signature in off line approach is complex because there is dynamic information is not available[1]. Offline signature approach is also difficulty because of highly stylish and unconventional writing styles. Signature also contain variation due to the nature and the variety of the writing pen which also increase the complexity of offline approach. Signature is affected by age, illness and geographic location, emotional state of signer. Due to this non-repetitive nature of variation in signature, there is large intra-personal variation.

In off line automatic signature verification system we need to deal with main two problem. Every off line verification system uses set of sample signature for training but in real time application it is very difficult to obtain large set sample signature from same signer for training our system. We need to reduce the requirement training set in our system. Another problem is that our system should be able to find out different type of forgeries.

Three type of forgery showed in literature are as follow[1]

1) **Random Forgery:** Random forgery can be considered as any signature other than author. In this type of forgery forger has no idea about shape of original signature.
2) **Simple Forgery:** In simple forgery forger has little idea about original signature. He/she create forge signature without much practice.
3) **Skilled Forgery:** In skilled forgery forger has full knowledge of original signature and enough time for proper practice.

Following metrics can be used for performance analysis.

1) **False rejection rate:** This represent the number of genuine signatures are rejected from tested total original signature.
2) **False Acceptance Rate:** This represent the number of forged signatures are accepted from tested total forged signature.
3) **Equal error rate:** Each verification system can be tuned to a level at which both accept and reject error rates are equal. This rate is called equal error rate.EER can be average of FAR and FRR.

   EER provides a quick way to compare the accuracy of verification systems. In general, a system with lower EER is considered to be more accurate.

II. LITERATURE REVIEW

A great deal of work has been done in the area of signature verification for the detection of random and skilled forgeries.. Some of them are discussed below:

In [1]optical flow to estimate local stability among signatures used. First optical flow is used to find a stability model of the original signatures for each signer. In the verification stage, the stability between the unknown signature and each one of the reference signatures is estimated and consistency with the stability model of the signer is evaluated.Optical flow vectors is used to detect the stable regions in the signature by analyzing the local stability of a signer.

In[3] For automatic signature verification process boundary and projection based global features are used. The total energy used for generating the signature is the first global feature. Information from the vertical and horizontal projections of a signature, the height or width of the signature, focusing on the proportion of the distance between key strokes in the image is used as the second feature. For offline signature verification the combination of these features with the ratio feature and the Modified Direction Feature (MDF) gives good results.For training support vector machine 12 original and 400 random signature is used

In [2] paper offline verification system analyze images of handwritten signature to find information about pressure distribution. histogram calculated from gray scale images is used as "spectrum" for computation of pseudo cepstral coefficients. For signature verification the unique minimum-phase sequence feature is used. The best possible number of pseudo coefficients is estimated for best system performance. The original and duplicate training samples has been randomly subdivided in two subsets of the same size (12 genuine and 12 forgeries). offline verification system trained by one subset. and for testing the offline verification system another subset will used. Remaining samples were used for verification.

In [4] offline signature verification is presented with set of geometric features of signature. In this method the features of signature that can differentiated between original and forge signature have been calculated using 16 bits fixed-point arithmetic. For testing offline verification system different classifiers HMM, SVM and Euclidean distance classifier is used. The results show that hidden markov model(HMM) works to some extent better than support vector machine(SVM) and the distance Euclidean verifier. Here 12 sample signature is used for training different classifier and for comparing result of different classifier.

In [5] method, local binary pattern(LBP) and local directional pattern(LDP) features to classify gray scale static signatures is used.The proposed method obtains eight gradient images from the gray scale static signature image. The local directional pattern image is obtained coding the eight gradient signature images. the discrete cosine transform(DCT) of a sequence obtained concatenating the histogram of the local directional pattern image blocks is used to calculate feature vector.

III. PROPOSED METHOD

Step 1: Pre-processing

In this step signature image processed for noise reduction, thinning.

A noise reduction filter is used in the binary image for removing single black pixels on white background.

Thinning is applied to eliminate the thickness differences of pen by doing the image one pixel thick.

Step 2: Feature Extraction

In this step features are extracted which have same variability for signer. general idea here is that we use more feature of available sample signature.

We use following features:

1)Signature area is found by calculating number of pixel in signature image. Signature area gives information about the density of signature.

2)Signature height-to-width ratio is obtained by dividing signature height to signature width. Signature height and width alone can change but Height-to-width ratios of one person's signatures are approximately equal.

3)Maximum horizontal histogram and maximum vertical histogram: The horizontal histograms are calculated for each row and the row with highest horizontal histogram value is taken as maximum horizontal histogram. The vertical histograms are calculated for each column and the column with highest vertical histogram value is taken as maximum vertical histogram.

4)Edge point numbers of the signature: Edge point is the pixel which has only one neighbor belonging to the signature, in 8-neighbor.

5)Optical flow vectors is used to detect the stable regions in the signature by analyzing the local stability of a signer. Optical flow shows the distribution of apparent velocities of movement and brightness patterns in an image.

6)The distribution of pixels is calculate by subdividing image into grid and counting how many pixels are expressed in the current subimage. This feature incorporates a static descriptor, which provides an insensitivity to intrapersonal variations.

7)The local binary pattern operator describes the surroundings of a pixel by generating a bit-code from the binary derivatives. The LBP operator takes the eight neighboring pixels using the canter gray level value as a threshold. The operator generates a binary code 1 if the neighbor is greater than or equal to the centre, otherwise it generates a binary code 0. The eight neighboring binary code can be represented by a 8-bit number. The LBP operator outputs for all the pixels in the image can be accumulated to form a histogram. For binary images, the LBP can be used for describing several structures as strokes ends, bifurcation, spots and other local features and its orientation.

Step 3: Training and Testing:

In this step we use support vector machine classifier. SVM is trained using feature vector from step 2 of available copy of genuine signature. To test originality of input signature, feature vector extracted from input signature is used as input for SVM. SVM will classify it either genuine or not. SVMs are very universal learners. Using set of examples from two classes as training, a support vector machine define the hyper plane, which have maximum the distance from either class to the hyper plane and separates the largest possible number of points belonging to the same class on the same side.

IV. EXPERIMENTAL RESULT

Off-line signature database contains data from 4000 synthetic individuals, 24 original signatures for each individual, and 30 forgeries of his/her signature. All the signatures were generated with different modeled pens. The signatures are in "jpg" format and equivalent resolution of 600 dpi.

Title of paper	Required Sample Signature for Training	EER(%)
Proposed Method	Minimum 3 genuine Signature and 100 Random forgery	13.0
Verification of Static Signatures by Optical Flow Analysis[1]	6 genuine Signature and 6 Skilled forgery	4.0
Offline Signature Verification Based on Pseudo-Cepstral Coefficients[2]	12 genuine Signature and 12 Skilled forgery	6.20
Signature Verification using Local Directional Pattern(LDP)[5]	5 genuine Signature and 99 Random forgery	9.02
Offline Signature Verification Using Classifier Combination of HOG and LBP Features[10]	12 genuine Signature P Random forgery(P not specified)	15.41
Global Features for the Off Line Signature Verification Problem[3]	12 genuine Signature and 400 Random forgery	17.25

V. CONCLUSION

Automatic Offline signature verification is very useful for identification. signatures is used in number of transactions, specially related to financial and business to verify originality of it. In this research we have tried to improve the performance in signature verification technique by using large number of feature for signature. In proposed method SVM is used for classification. In proposed method 3 genuine signature and 100 randomly forged signature is used for testing and give 13% EER.

REFERENCES

[1] G. Pirlo and D. Impedovo “Verification of Static Signatures by OpticalFlow Analysis” IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 43, NO. 5, SEPTEMBER 2013

[2] Jesus F. Vargas Miguel A. Ferrer, Carlos M. Travieso, Jesus B. Alonso “Offline Signature Verification Basedon Pseudo-Cepstral Coefficients” 2009 10th International Conference on Document Analysis and Recognition

[3] Vu Nguyen, Michael Blumenstein Graham Leedham “Global Features for the Off-Line Signature Verification Problem” 2009 10th International Conference on Document Analysis and Recognition

[4] Miguel A. Ferrer, Jesu´s B. Alonso, and Carlos M. Travieso “Offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic” IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 27, NO. 6, JUNE 2005

[5] Miguel A. Ferrer, Francisco Vargas, Carlos M. Travieso, Jesus B. Alonso “Signature Verification using Local Directional Pattern (LDP)” Security Technology (ICCST), 2010 IEEE International Carnahan Conference on

[6] Oliveira, L. E. S., Justino, E., Freitas, C. O. A., Sabourin, R. "The Graphology Applied to Signature Verification". In: 12th Conference of the Internatioal Graphonornics Society, 2005, Salerno.

[7] K. W. Boyer, V. Govindaraju, and N. K. Ratha, Eds., “Special issue on recent advances in biometric systems,”IEEE Trans. Syst., Man Cybern. B, vol. 37, no. 5, pp. 1091–1095, Oct. 2007

[8] D. Impedovo and G. Pirlo, “Automatic signature verification — the state of the art,”IEEE Trans. Syst., Man Cybern. C, Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep. 200

[9] Heinen, M. R.; Osorio, F. S. "Handwritten Signature Autentication using Artificial Neural Network". In: IJCNN - IEEE Intenational Joint Conference on Neural Networks, 2006, Vancouver. Proceedings of the WCCI (World Congress on Computational Intelligence) - IJCNN.Vancouver - Canada : IEEE Press, 2006. v. 1. p. 10 111-10118.

[10] Mustafa BerkayYilmaz, Berrin Yanikoglu, Caglar Tirkaz Alisher Kholmatov “Offline Signature Verification Using Classifier Combination of HOG and LBP Features” Biometrics (IJCB), 2011InternationalJointConferenceon Biometrics Compendium, IEEE