Implementation of offline Signature Verification System by using Grid Based Feature Extraction

Urmila A. Jain
P.G. Student
Department of Computer Engineering
R.C. Patel Institute of Technology,
Shirpur, Dist: - Dhule, Maharashtra, India.

Prof. Nitin N. Patil
Head &Associate Professor,
Department of Computer Engineering
R.C. Patel Institute of Technology,
Shirpur, Dist: - Dhule, Maharashtra, India..

***Abstract*—Signature verification (SV) is one of important and useful biometric authentication method. Offline SV detects whether signature is original or fake. This method uses four steps Signature acquisition, pre-processing, feature extraction and verification. The discussed system uses grid features. For verification, the extracted features of test signature are compared with already referenced features of reference signature. The threshold used can be dynamically changed according to the application.**

Keywords—Biometry, Forgery, Signature Verification, FRR (False Rejection Rate), FAR (False Acceptance Rate), SVM (Support Vector Machine), HMM (Hidden Markov Model), NN (Neural Network).

INTRODUCTION

Signatures are most commonly used by people in their daily life and are most useful way of legal identity of individual. Many times in several applications these signatures are used as a means of identity verification. It is used in many applications like legal applications, banking and in highly secured environments [1], so such application requires their own software to perform signature verification. These signatures are made up of different symbols and letters. Each person has its own way of making signatures so these signatures are not just combination of letters but it looks like some image with different curves and strokes at different places. So it is today's need to identify that signature is genuine or forgery. There are some techniques that can also be used for identity verification like password. But passwords are not unique and can be easily stolen or lost or broken. In case of biometric authentication, every person have unique biometric characteristic so they can't be easily stolen or lost therefore it is better means of security than password. Signature has been a distinguishing feature for person identification. Even today numbers of transactions, especially related to business and financial are being authorized via signatures. Therefore there is need to have methods of automatic signature verification must be developed if authenticity is to be verified and guaranteed successfully on a regular basis. Signature verification is divided into two categories depending on how that is acquired for purpose of verification [2].

1. Offline Signature verification
2. Online signature verification.

1. **Offline signature verification:** In the offline signature verification, signatures are written on paper and are acquired through scanners in electronic form or in image. In this case, we have just static information of signature means just features of signatures. Since only static information is available, signatures are difficult to forge.
2. **Online Signature verification :** In online verification method , the signature is acquires during the writing process of signature, a signature data can be obtained from an electronic tablet and in this method, dynamic information of signature about writing process such as pressure applied ,speed of writing , angle and direction of the pen are available and numbers of strokes. In this case, forgeries are easy to detect.

The paper presents the method of offline signature verification.

Offline Signature Verification Concepts

We know the fact that no two signatures are never same, even if they are signed by the same person. However, even though two signatures are *exactly same*, then one of them is not an original signature but is a duplicate copy of the other that may be a machine copy for e.g. one produced by a photocopier, computer or a manually produced copy by tracing. So the aim of the signature verification system is to classify between two types: the original and the forgery. These classifications are related to intrapersonal variability and interpersonal variability. The variation of signatures of same person is called Intrapersonal Variation. The variation between genuine/original and forgeries is called as Inter Personal Variation.

Forgery means that some person is trying to make false signature of some another person for authentication purpose. Forgeries are classified into three types [5]:

Forgery Types

In signature verification techniques, fake/forged signatures can be divided into three types. These types are based on how similar a forge signature is to the genuine/original signature and are known as random forgery, simple forgery and skilled forgery. A random forgery is the one in which the forger/writer does not know the signature shape. He is just making any signature knowing only name. A simple forgery is that forger knows the name of the original writer/signer and how their signature looks like but he is not well practiced. He just makes the signature by just seeing it once. A skilled forgery is a close to the genuine signature and is made by a forger/writer who has seen and well-practiced writing the original/genuine signature.

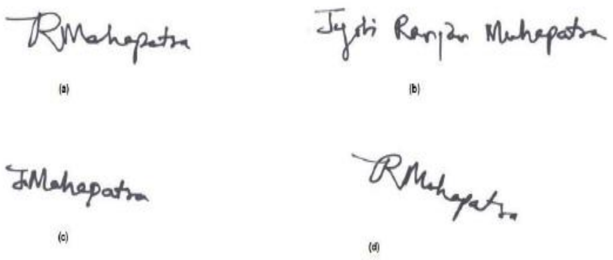


Fig . 1. Types of Forgery (a). Original Signature (b). Random Forgery (c). Simple Forgery (d). Skilled Forgery

LITERATURE SURVEY

A lot of research has been done on offline signature verification. In [3] signature verification is proposed by A. Rathi et al. which is pixel based method. This method gives higher FRR and lowers FAR due to which systems performance degrades. In [4], Julian Fieerez proposed the method for offline signature verification that is based on counter features. In [5] each pixel of the input signature has been studied and the end points of the signature were extracted. Verification is based on structural features such as perimeter, circulatory measure, area, rectangularity measure and minimum enclosing rectangle. In [6] Priyanka Chaurasia proposed a verification technique that uses local and global feature extraction in regions of high pressure of an image. In the said method, all verification has been carried on skilled forgeries.

Following Fig. 2 shows process of a signature verification system [7]. The process follows the classical pattern recognition model steps like data acquisition, preprocessing, feature extraction, verification and performance evaluation.

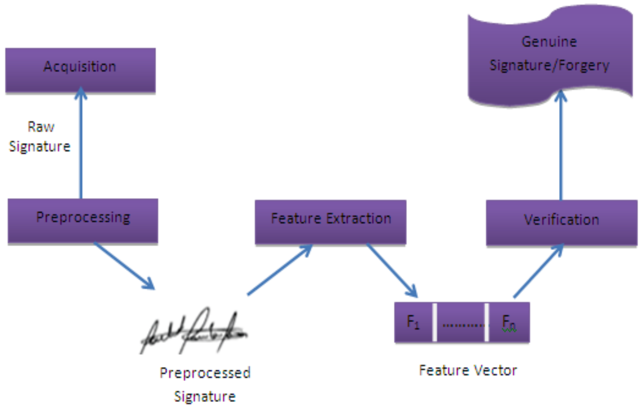


Fig. 2 General Signature Verification System

IMPLEMENTATION

An offline signature verification method consists of following steps[1]:

1. Signature Acquisition
2. Signature Preprocessing
3. Feature Extraction
4. Signature Verification

A. Signature Acquisition: In this step, Signatures are made followed by scanning and storing. Fig.3 shows some of the sample signatures from CEDAR database on which the proposed scheme has been tested.

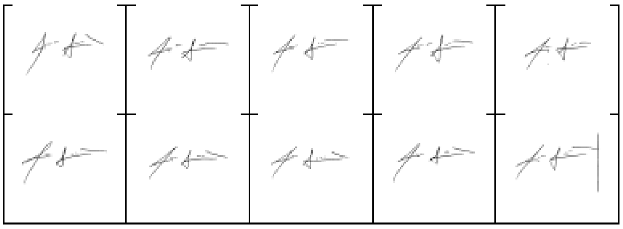


Fig. 3 sample signatures

Fig 4 shows the image given as input to the system.

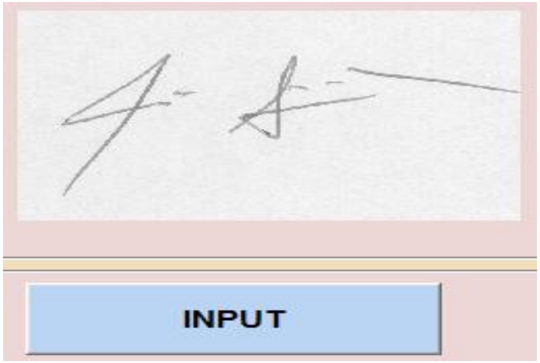


Fig 4 Input signatures

B. Signature Preprocessing: In this step to verify a signature correctly, acquired signatures are preprocessed. The signature image shown in Fig.4 may sometimes contain extra noise. It is essential to remove these extra noises from image for correctly verifying the signature.

In the data preprocessing phase, the input data is enhanced. It includes [8]:

a) Data Area Cropping: In this, initially the original color image is segmented from its background to remove the extra white space surrounding the signature using the various segmentation methods of horizontal and vertical projections.

b) Binarization: The color signature is converted to gray-scale image and then finalized using the some histogram-based binarization algorithms.

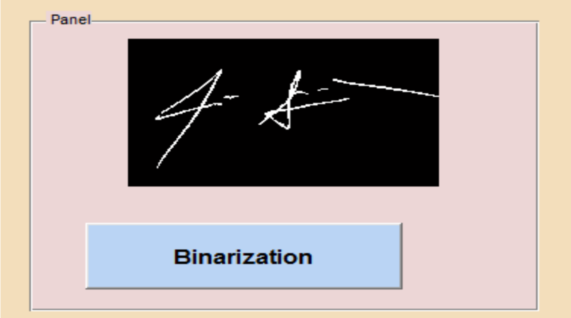


Fig 5: Signature after preprocessing

C. **Feature Extraction:** The main objective of this phase is to extract the grid features of the test image and those will be compared with the features of trained image for verification.

After preprocessing a signature, a grid of m x n is formed. Fig. 6 shows the grid corresponding to above input image. Therefore, a signature image is divided into 200 square cells such that each cell is having 100 pixels.

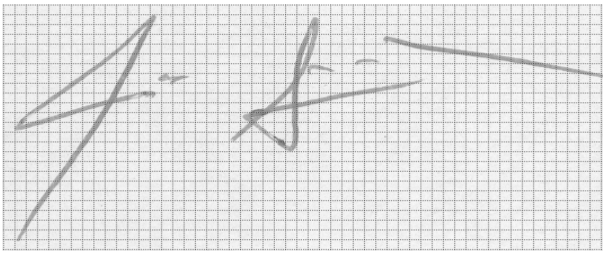
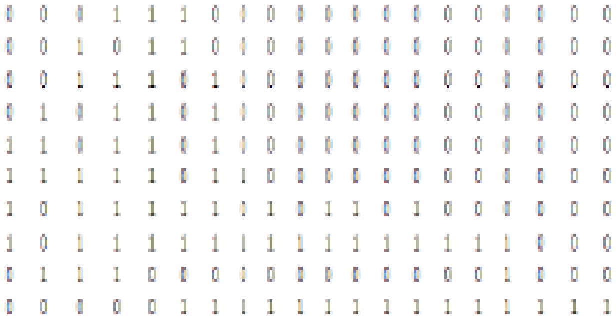


Fig.6. Grid over pre-processed signature image

Now the signature content will be considered as black pixels with value 1 otherwise 0. The cells of a row of a grid that are containing the signature content are calculated. The process is repeated for all rows of a grid. Thus we will have a matrix of size *m* x *n* corresponding to the grid of size *m* x *n*.As a result of this step, we will have a matrix of elements 0 or 1 as shown in fig. 7.As we calculated the row matrix, we will calculate column matrix. The cells of a column of a grid that are containing the signature content are calculated. The process is repeated for all columns of a grid. Thus we will have a matrix of elements 0 or 1.



0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Fig.7. Matrix corresponding to above grid

Here three features extracted are: (i) a*m* x *n* matrix that corresponds to a*m* x *n* grid of image. (ii) an array of size *m* in which first element gives the number of black pixels that are in first row of a grid, second element gives the number of black pixels that are in second row and so on; (iii) an array of size *n* in which the first element gives the number of black pixels that are in first column of the grid, second element gives the number of black pixels that are in second column and so on[1].

These features are used in verification process. These features are compared with reference signature images and then classified them as genuine or forge. The verification process is as shown in following fig 3[1]. In verification process, both reference array and test array are compared and CMS(Column Matching Score) and RMS(Row Matching Score) are calculated. Based on the values of CMS, RMS and threshold the signature is classified as forgery and original.

D. **Signature Verification:**The purpose of verification phase is to compare and verify the test image with the training image using extracted features and also to decide whether the given test image is original or forgery.

Steps for Verification

(a) Calculate CMS(Column Matching Score)

(i) Let $M_{1,}$ M_2 be the matrices for reference image and input/test image respectively. The columns of matrix $M_2$is compared with M_1. Each column is having *m* elements. If at least βelements are same, where $\beta \geq 7$, then that column is said to be matched with reference imageandthe column count $C_1$is increased by one.

(ii) Now, Let A_1 and A_2 are the arrays of reference image and input/test image respectively that are containing number of black pixels ineach and every column. Compare these corresponding elements of A2 with A_1 and check the following condition:

$$\sigma_{Ref} - \alpha < \sigma_{Test} < \sigma_{Ref} + \alpha \qquad (1)$$

where, $\sigma_{Ref}$is element of reference array A_1 and$\sigma_{Test}$is corresponding element of test array A_2 and α is tolerable factor which is the allowed variations in number of pixels. It is a dynamic value as it always varies for different columns based on the signature content in that column.

(iii) If C1 = n and C2 = n, then column Matching Score (CMS) is said to be 100%.

Same for C1 = n-i and C2 ≥ n-i where i=1,.....,8, CMS will be $\frac{n-i}{n} * 100$ % that means signatures up to 60% Column Matching Score(CMS) are considered for further processing but If Column Matching Score(CMS) is below 60% then test signature will be classified as fake/forgery at this step itself.

(b) Calculate Row Matching Score (RMS)

If CMS ≥ 60% then and only then we will calculate Row Matching Score (RMS) and it can be obtainedsimilarly as CMS. All the comparisons are done row wise. For RMS(Row Matching Score), β ≥ 14. Then calculate C1 and C2 for this case.

(c) Calculate Average of Column Matching Score(CMS) and Row Matching Score(RMS).

(d) Threshold

Here we are considering the threshold as the security level which user wants to achieve in target application. If the user wants total 100% security, then input will be 100 and if the average of the Column Matching Score and Row Matching Score is 100% then the input signature will be accepted.

signature original

Fig. 8 Message box showing signature original or forgery

The Fig. 9 shows the verification technique proposed in this paper

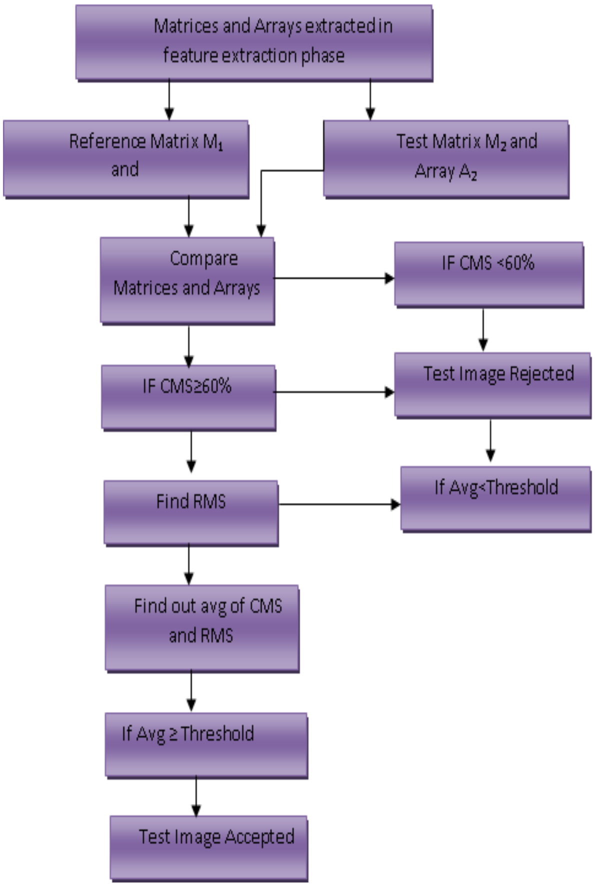

Matrices and Arrays extracted in feature extraction phase
Reference Matrix M_1 and
Test Matrix M_2 and Array A_2
Compare Matrices and Arrays
IF CMS <60%
IF CMS≥60%
Test Image Rejected
Find RMS
If Avg<Threshold
Find out avg of CMS and RMS
If Avg ≥ Threshold
Test Image Accepted

Fig 9: Proposed Verification Scheme

EXPERIMENTAL RESULTS

The performance of this method is measured in terms of FAR and FRR [1].

FAR(False Acceptance Rate) is calculated as total number of forged signatures accepted by total number of comparison of signatures made.

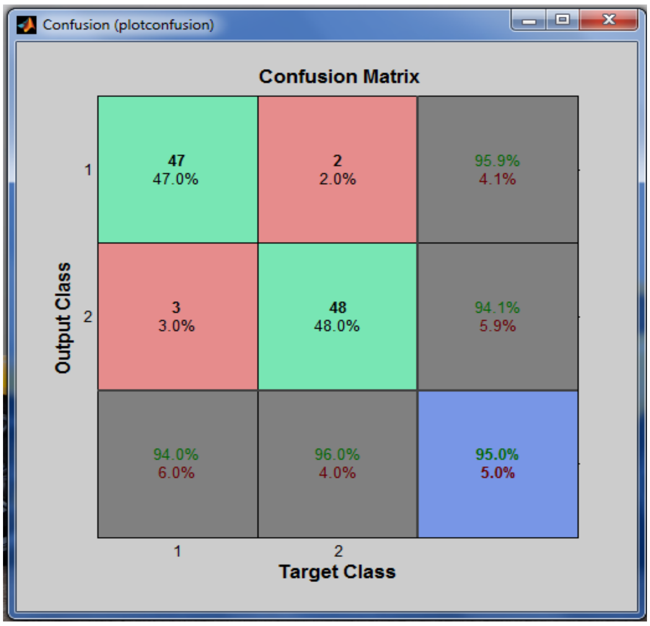
$$FAR = \frac{No.of\ forgeries\ accepted}{(No.of\ forgeries\ tested)} * 100$$

FRR(False Rejection Rate) is calculated as total number of original signatures rejected by total number of comparison of signatures made.

$$FRR = \frac{No.of\ genuines\ rejected}{(No.of\ forgeries\ tested)} * 100$$

We have calculated FAR and FRR to evaluate the performanceof the proposed system. The confusion matrix is shown fig. 10.

The experimental results are shown with the help of confusion matrix. The FAR is 4.1%. The FRR is 5.9%.



Confusion Matrix

Output Class	Target Class 1	Target Class 2	
1	47 47.0%	2 2.0%	95.9% 4.1%
2	3 3.0%	48 48.0%	94.1% 5.9%
	94.0% 6.0%	96.0% 4.0%	95.0% 5.0%

Fig. 10 Confusion Matrix

CEDAR DATASET

TheCEDAR(Center of Excellence for Document Analysis and Recognition) signature dataset is a most commonly used dataset for off-line signature verification. This dataset contains 55 signature sets, each set being formed by one writer. Each writer has given 24 samples of their signature which are genuine. The forgeries were asked by random people to forge the signatures of the previously given writers. Like way, 24 forgery samples were collected for each writer from near about 20 forgers which were trained skillfully. So, this dataset contains total 2,640 signatures out of which 1,320 are genuine and 1,320 are forgeries signatures, which are of the skilled type. Fig 11 and fig 12 shows an sample example of genuine/original signatures and forgery signatures.

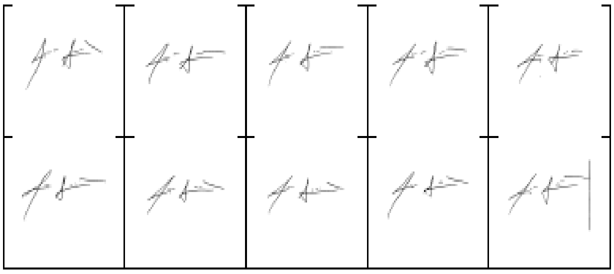


Fig. 11: genuine samples for one writer

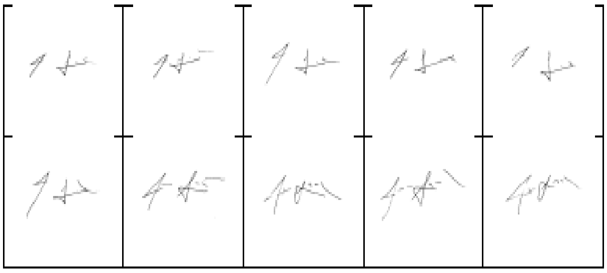


Fig. 12: forgery samples for the same writer in Figure 11

CONCLUSIONS

In this paper, we discussed an offline signature verification method by using grid based feature extraction. The signature is acquired in image form and then preprocessed using binarization. The preprocessed signature is converted into grid then the matrix corresponding to that grid is formed and then arrays containing number of black pixels in columns and rows formed. For verification, these two row and column arrays for training and test images are compared, both row wise and column wise and then the test signature is classified accordingly. This method gives comparatively better results. The FAR and FRR are also less as compared to existing approaches. The existing grid based feature extraction method was having FAR 13.5 and FRR is 10.8 which are much more as compare to this. It was having higher probability of rejecting genuine signature and accepting forgery signature.

REFERENCES

[1] Swati Srivastava, Suneeta Agarwal, “Offline Signature Verification Using Grid Based Feature Extraction”, *in International Conference on Computer & Communication Technology (ICCCT)*, IEEE, pp. 185-190, 2011

[2] A. A. Zaher and A. Abu-Rezq, “A Hybrid ANN-Based Technique for Signature Verification”, *Proceedings of the 4th WSEAS International Conference on COMPUTATIONAL INTELLIGENCE*, Universitatea Politehnica, Bucharest, Romania, April 20-22, 2010, pp. 13-19.

[3] A. Rathi, D. Rathi and P. Astya, “Offline handwritten Signature Verification by using Pixel based Method”, International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 7, pp. 1-4, September – 2012.

[4] A. Gilperez, F. Alonso-Fernandez, S. Pecharroman, J. FiEERez, and J. Ortega-Garcia, “Off-line signature verification using contour features,” Proc. ICFHR, 2008.

[5] Debasish Jena, Banshidhar Majhi, Saroj kumar Panigrahy, Sanjay Kumar Jena, “Improved Offline Signature Verification Scheme Using Feature Point Extraction Method”, Proc. 7th IEEE Int. Conference. on Cognitive Informatics, pp. 475 – 480, ICCI 2008.

[6] Priyanka Chaurasia, “Offline Signature Verification using High Pressure Regions”, Patent No. US 7,599,528 B1, 2009.

[7] Launa Batista, Dominique Rivard, Robert Saobourin, Eric Granger, Patrick Maupin, “State the Art in Off-Line Signature Verification”, 2008, pp-40-62.

[8] M. Arya and V. Inamdar, “A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches”, International Journal of Computer Applications, vol. 9, pp. 77-83, 2010

[9] Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing, “Offline Signature Identification by Fusion of Multiple Classifiers using Statistical Learning Theory”, Computer Vision and Pattern Recognition, IJSIA 2010.

[10] Urmila Jain, Prof. Nitin N. Patil, “A comparative study of various methods for offline signature verification ", International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT-2014), IEEE, pp. 760-764, Feb-2014.