AN APPROACH FOR OFF-LINE SIGNATURE VERIFICATION SYSTEM USING PEAK AND CURVE COMPARISON

Abu Shamim Mohammad Arif, Md. Sabbir Hussain, Md. Rafiqul Islam, S. A. Ahsan Rajon and Abdullah Al Nahid

Abstract— A great deal of work has been done in the area of off-line signature over the past two decades. Off-line systems are of interest in scenarios where only hard copies of signature are available, especially where a large number of documents need to be authenticated. But Signature verification is still now difficult task. Recognizing color image of signature and rotational displacement of same person's signature are major problems. We have solved this problem using some techniques because no single algorithm is sufficient to recognize a hand written signature properly. Here we have used new technique of curve matching for comparing two signatures. The curve generated in this procedure has been compared with the curve of the signatures generated in same way stored in the database. For rotational displacement we normalize each signature with respect to rotation. The signature's scanned portions are cut and stored as JPEG format in 100x100 pixels. The signature is then converted into matrix form and represented into viewer as collection of pixels. Then signatures are processed with skeletonization, rotation, translation, peak detection and comparison and curve matching. We take several portions of curve with respect to peak and compare the same portion with others. The outcomes of different phases are stored in database. Curve matching can significantly improve verification rate. Accuracy of our system is calculated by False Acceptance Rate (FAR) and False Rejection Rate (FRR) are 1.38 % and 13.75% respectively.

Index Terms—Curve matching, Off-line signature, Peak detection, Signature verification.

1 INTRODUCTION

SIGNATURE verification system is very important research area to verify individual's identity. Signature verification is a process in which the signature of an individual is verified whether the signature belongs to the claimed person or not. It is a technique that finds for each sample in one of the signatures, the corresponding sample in the other signature that is closest to the original sample using some predefined metrics. The error of the verification algorithm is estimated using a technique that overcomes the small number of example signatures and forgeries provided by the subjects. The performance of a verification system is generally evaluated according to the error rate representation of pattern recognition problem. We can generally distinguish between two different categories of verification system - Online and off-line. For online, the signature is captured during the writing process, thus making the dynamic information available and off-line for which the signature is captured once the writing processing is over and, thus only a static image is available[3]. The objective of signature verification system is to discriminate between two classes:

The original and the forgery, which are related to intra and interpersonal variability. The variation among signatures of same person is called intra personal variation. The variation between originals and forgeries is called inter personal variation [2].

Types of Forgeries

There are three different types of forgeries to take into account. The first, known as random forgery which written by the person who don't know the shape of original signature. The second, called simple forgery, is represented by a signature sample which written by the person who know the shape of original signature without much practice. The last type is skilled forgery, represented by a suitable imitation of the genuine signature. Each type of forgery requires different types of verification approach. Hybrid systems have also been developed. Fig. 1 shows the different types of forgeries and how much they vary from original signature.

- *Abu Shamim Mohammad Arif is with Computer Science and Engineering Discipline, Khulna University, Khulna-9202, Bangladesh. E-mail: shamimarif@yahoo.com.*
- *Md. Sabbir Hussain is with Computer Science and Engineering Discipline, Khulna University, Khulna-9202, Bangladesh. E-mail: sabbir_2196@yahoo.com.*
- *Md. Rafiqul Islam is with Computer Science and Engineering Discipline, Khulna University, Khulna-9202, Bangladesh. E-mail: shohag_05@yahoo.com.*
- *S. A. Ahsan Rajon is with Computer Science and Engineering Discipline, Khulna University, Khulna-9202, Bangladesh. E-mail: ahsan.rajon@gmail.com*
- *Abdullah Al Nahid is with Electronics and Communication Engineering Discipline, Khulna University, Khulna-9202, Bangladesh. E-mail: nahidku@yahoo.com*

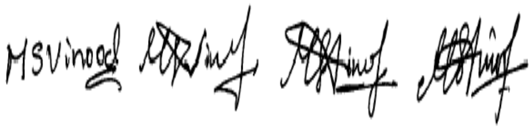


Fig. 1. Different types of forgeries

Noise

Noise is a random error in pixel value, usually introduced as a result of reproduction, digitalization and transmission of the original image. Noise cannot always totally be eliminated, but smoothing is widely used.

Peak

Peak detection is one of the most important time-domain functions performed in signal monitoring. Peak detection is the process of finding the locations and amplitudes of local maxima and minima. We can perform peak detection, such as threshold peak detection and curve-fitting-based peak detection. Here we used the Curve fitting based pick detection.

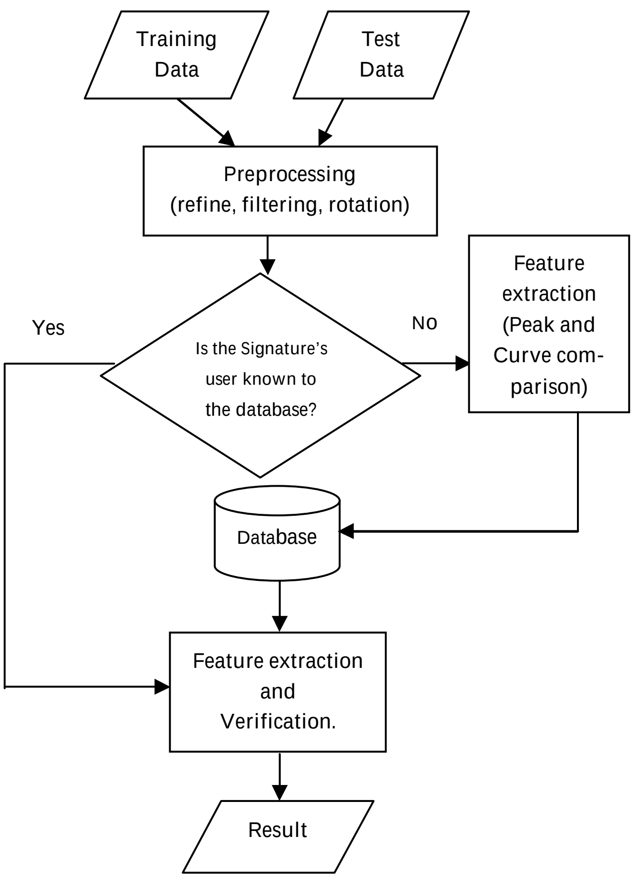


Fig. 2. Flow-chart for handwritten signature verification

2 PREPROCESSING

Scaling

For the variation of signature length in the test and training signature, the signatures need to be scaled [1]. If H_I and W_I are the height and width of the image then we can make the image at uniform 100x100 pixels by the simple equations.

$$X_{new} = X_{old} * S_x$$

Where Sx=100/H_I; X is any horizontal unit and is the horizontal scaling factor.

$$Y_{new} = Y_{old} * S_y$$

Where Sy=100/W_I; Y is any vertical unit and is the vertical scaling factor.

Loading Image

The signature is then converted into matrix form and represented into viewer as collection of pixels. The Refining and filtering step is known as skeletonization [9]. Here refining step is done in two steps and filtering step is done in four steps.The image is loaded according to the colour of every pixel. Signature may be written in black colour in white page. If we represent the colour in RGB (Red, Green, Blue) format then for black colour we get the following format-
R=0, G=0, B=0. And white colour format is R=255, G=255, B=255.

When it is taken into 100x100 matrix the white colour (255,255,255) is taken as value '0' and black colour is taken as value '1'. When signature is represented in the screen then value '1' is represented as 'o' that can be said as pixel and value '0' is represented as ' '. The main idea is that the colour says RGB (240,240,240) & colour RGB (255,255,255) are looks quite similar (white).

Skeletonization

A simplified version of the skeletonization technique described by Lam and Suen is used. The simplified algorithm used here consists of the following three steps:

Step 1: Mark all the points of the signature that are candidates for moving (black pixels that have at least one white 8-neighbor and at least two black 8-beighbors pixels).

Step 2: Examine one by one all of them, following the contour lines of the signature image, and remove these as their removal will not cause a break in the resulting pattern.

Step 3: If at least one point was deleted go again to Step 1 and repeat the process once more.

Fig. 3. shows an example of this skeletonization technique. Skeletonization makes characteristics like the qualities of the pen and the paper the signer used, and the digi-

tizing method and quality.

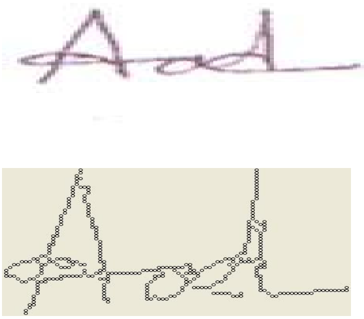


Fig. 3. Example of the skeletonization

Rotation

To perform rotation [7], normalization, the signature curve was rotated until the axis of least inertia coincided with the horizontal axis. To achieve this, the following procedure was followed

We represented the given signature curve, C as shown in (1).

$$C = \{ x(i) = \begin{bmatrix} u(i) \\ v(i) \end{bmatrix}, i = 1, \ldots\ldots, N \} \quad (1)$$

Where,
C = signature curve,
N = Number of pixels in the signature,
X(i) = Vector consisting of x- and y- coordinates of the ith pixel in the signature,
u(i) = x- coordinate of the ith pixel in the signature curve,
v(i) = y- coordinate of the ith pixel in the signature curve.

Next, we found the coordinates, u and v of the center of mass of the signature.

$$\bar{u} = \frac{1}{N}\sum_{i=1}^{N} u(i), \qquad \bar{v} = \frac{1}{N}\sum_{i=1}^{N} v(i). \quad (2)$$

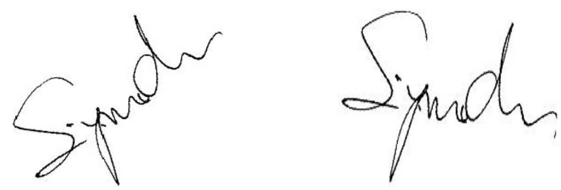
We then calculated the second order moments u2 and v2 of the signature by (3).

$$\overline{u^2} = \frac{1}{N}\sum_{i=1}^{N} (u(i) - \bar{u})^2, \qquad \overline{v^2} = \frac{1}{N}\sum_{i=1}^{N} (v(i) - \bar{v})^2. \quad (3)$$

The orientation of the axis of least inertia was then given by the orientation of the least given vector of the matrix in (4)

$$I = \begin{pmatrix} \overline{u^2} & \overline{uv} \\ \overline{uv} & \overline{v^2} \end{pmatrix}. \quad (4)$$

Once this angle was obtained, all the points in the signature curve under consideration were rotated with this angle.



(a) (b)

Fig. 4. : Rotation: (a) Original (b) After rotation and normalizing

3 Proposed Method

Feature Extraction And Reduction

A fundamental process in any recognition system is the feature extraction. The objective here is to capture the essential characteristics of the patterns. A feature is a function of one or more measurement, computed so that it quantifies some significant characteristics of the object.

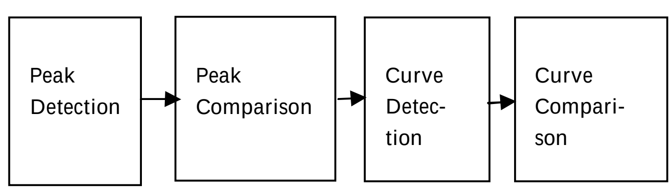


Fig. 5. Peak and Curve detection and comparison

Obviously feature reduction is a sensitive procedure since if the reduction is done incorrectly the whole recognition system may or not produce the desired result. Here we establish a technique of comparing two curves. This is done in several phases such as peak detection and comparison, curve detection and curve matching. After detecting the curves, we compare the same portion with others. The outcomes of different phases are stored in database.

Peak Detection

Peak is one of the most important identifying features of any signature. Every signature must contain peak. The height of peak may be high or low. Peak of a signature can be detected by evaluating its height with respect to y axis and ground. The height is measured in such a way that if the signature is considered as a hill and one walk upon that hill and come down to ground. Then the height of the hill is detected and this height is the peak height. This value is set at the peak and the x and y value of that point is recorded for next step. This process is done for both up-side view and down-side view. The algorithm and procedure is shown below.

Algorithm of peak detection for up side view:-
Peak()
//suppose X[][] be the matrix from where we detect peak output is taken to another matrix
//if a pixel is traversed then it is marked
//initially height=0
Begin:

1. Find a pixel which is not marked and X[i-1][j-1]=0 and X[i][j-1]=0 and X[i+1][j-1]=0 and X [i+1] [j] =0 where i & j starting form 0 to 100.
2. If such pixel found, then this is the starting pixel and traverse according to highest priority, mark previous pixel and call del(i, j).
   a. Increase height when new steps for y axis.
   b. Allow to move eight adjacent priority '8' condition and four adjacent priority '4' condition.
   c. If X[i+1][j-1]=1 or condition 'b' fails and height >15 then starting pixel = height and goto step1.
3. If no such pixel found then return.

End.

The function del used to delete the point backward from the current position.

```
Del (curx, cury){
  For(i=curx;i>=0;i--)
        X[i][cury]=0;
 }
```

The same algorithm in reverse order is used for the downside view.

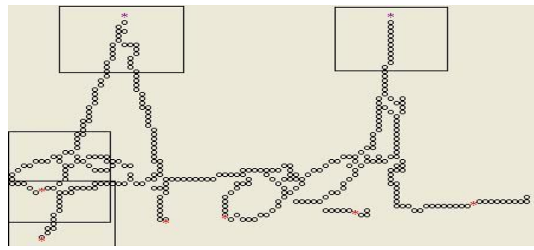


Fig. 6. Peak Detection

Peak Comparison

One of the most sensitive parts is the peak comparison. The most important part of peak comparison is that we have to guarantee that, we must compare the same peak with others. After filtering process the angle of rotation is obtained. Then original signature is rotated and then translating the signature to fit them to a certain fixed region in the matrix for comparison. After finishing this process peak comparison starts.

First step of peak comparison is the counting of peak for the upside view and peak for downside view. We compare the number of peak of upside view for input image and training image. We again compare the number of peak of downside view for input image and training image. A rule is followed that shown in table I. If the number of peak for input image and training image follows any one of that rule then testing signature is accepted otherwise rejected. The accepted signature is then stored in database and that is used for the next step. We need to mention that we must take that peak for this process which has height greater than 15 for input image and consider height greater than 13 for training image.

TABLE I
RULES FOR ACCEPTING AN IMAGE

Peak	
No. of peak for input image	No. of peak for training image
2	1 to 3
3	2 to 5
4	At least 3
5	At least 3
1	At most 2

Curve Detection

In the last phase of comparison we compare the certain portion of the curve with the similar portion of the same curve in a certain region. The detection of portion is not so tough but main problem arise to select the same portion of two signatures. This portion is selected from the peak that we did previously. From the curve around the peak point we take a region of width of 10 pixels and height of 10 pixels and the curve of that region is taken for compare. This is done for both testing signature and training signature. Starting from x=0 we move to x=100 and taking this curve and compare with that curve of other signature.

Curve Comparison

Suppose an equation of a curve of order two be

$y = ax^2 + bx + c$ Here Polynomial Regression procedure is used to find out second order polynomial curve equivalent to signature and to calculate a, b, and c values of that curve. The least square procedure can be used to an m-th degree order [11] of curve by the following equation.

$$y = a_0 + a_1 x + a_2 x^2 + \cdots\cdots + a_m x^m \qquad (5)$$

And the residuals

$$S = \sum (y_i - a_0 - a_1 x_i - a_2 x_i^2 - \cdots\cdots\cdots - a_m x_i^m) \qquad (6)$$

Where i = 1 to n

The value of $a_0, a_1, a_2 \ldots\ldots\ldots\ldots\ldots\ldots a_m$ can be determined as-

$$\frac{ds}{da_0} = -2\sum (y_i - a_0 - a_1 x_i - a_2 x_i^2 - \cdots - a_m x_i^m) \qquad (7)$$

$$\frac{ds}{da_1} = -2\sum x_i (y_i - a_0 - a_1 x_i - a_2 x_i^2 - \cdots - a_m x_i^m) \qquad (8)$$

$$\frac{ds}{da_2} = -2\sum x_i^2 (y_i - a_0 - a_1 x_i - a_2 x_i^2 - \cdots - a_m x_i^m) \qquad (9)$$

……………………………………………………………

$$\frac{ds}{da_m} = -2\sum x_i^m (y_i - a_0 - a_1 x_i - a_2 x_i^2 - \cdots - a_m x_i^m) \qquad (10)$$

Setting this derivatives equals to zero will result minimum m. We used order up to 2, i.e. our signatures reduce to a second order polynomial curve. Using polynomial regression, polynomial equation reduces to

$$a_0 * n + a_1 * \sum x_i + a_2 * \sum x_i^2 = \sum y_i \qquad (11)$$

$$a_0 * \sum x_i + a_1 * \sum x_i^2 + a_2 * \sum x_i^3 = \sum x_i * y_i \qquad (12)$$

$$a_0 * \sum x_i^2 + a_1 * \sum x_i^3 + a_2 * \sum x_i^4 = \sum x_i^2 * y_i \qquad (13)$$

Where all summations are from i=1 through n. We calculated the values of using Gauss Elimination method and stored these 's value for training pattern in database and later on for test the new pattern , we used these with the new ao,a1,a2 and the error rate calculation gives the result of comparison. If we consider the value of y can be learned as $y = \sum \left(a x_i^2 + b x_i + c \right)$, the value of y for two signatures then compared to find error.

4 RESULTS

For this verification system, signatures are collected from several persons. Ten signatures are taken form every person. One hundred people participated in this experiment. One signature of each person that is hundred signatures stored in database and the rest signatures are used for testing to find correspondence with the signatures stored in database. The main source of failure may be due to unavoidable noise present in the scanned image. It is difficult to extract the curvature [10] features from signature image, but such feature can significantly improve verification rate.

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the two parameters using for measuring performance of any signature verification method [5]. FAR is calculated by (14) and FRR is calculated by (15).

FAR = (number of forgeries accepted) / (number of forgeries tested) * 100 (14)

FRR = (number of originals rejected) / (number of originals tested) *100 (15)

The verification results for different values of the threshold were noted. As seen from the table, as the threshold increases, the FAR decreases, while the FRR increases, the corresponding results are shown below.

Threshold	0.01	0.10	0.20	0.50
FAR (%)	5.68	2.47	1.38	0.28
FRR (%)	2.85	13.32	13.75	20.24

The FAR for this method is 1.38% while the FRR is 13.75%.

Table shows the False Acceptance Rate of our method for different types of forgeries

Forgery Type	FAR (%)
Random Forgeries	1.38
Simple Forgeries	5.20

Table shows the False Rejection Rate for original signature.

Signature	FRR (%)
Original Signatures	13.75

Comparison

It is difficult to compare the performance of different signatures verification systems because different systems use different databases. Here we just list the performance achieved by some of the other system and that achieved by our system. We collected signatures [15] in order to evaluate the performance of the signature verification system. The data set consists of signatures from 100 subjects, each of them was asked to provide ten signatures, one to be used as the training set and the other to be used as the test set The Artificial Graphometric Features [1] which reports 6% FAR and 18% FRR only for simple forgeries. Again another paper, Novel Features [5] which reports 2.08%, 9.75%, 16.36% FAR for random, simple and skilled forgeries respectively and their FRR is 14.58%. Comparison has shown in the following graph.

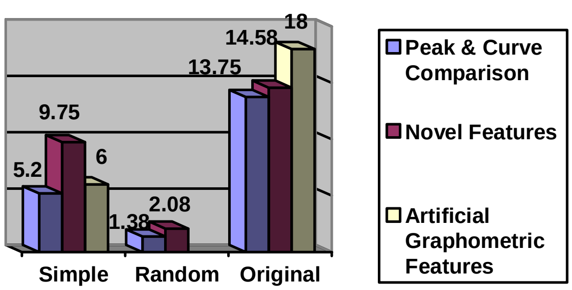


Fig. 7. Comparison Graph

From the above graph, we can see that our method shows better result than Novel Features [5] and Artificial Graphometric Features [1] for random and simple forgeries.

5 Conclusion

Our system has improved the signature verification process with rotation consideration. Here we have used new technique of curve matching for comparing two signatures. The curve generated in this procedure has been compared with the curve of the signature comes in same way stored in database. For rotational displacement we normalize each signature with respect to rotation. The signature portions then cut and stored as JPEG format in 100x100 pixels. The signature then converted into matrix form and represented into viewer as collection of pixels. Then signatures are processed with skeletonization, rotation and translation. The verification process is done in several phases such as peak detection and comparison, curve detection and curve matching. We take several portions of curve and compare the same portion with others. The outcomes of different phases are stored in database. Curve matching can significantly improve verification rate.

References

[1] Hasan Al Noor, Mahbub Murshed, Saifur Rahman, 2003, "Handwritten signature verification system using artificial graphometric features", ICCIT-2003.

[2] Migual A.Ferrer, Jesus B. Alonso and Carlos M. Travieso, 2005, "Off-line geometric parameters for automatic Signature Verification Using Fixed-Point Arithmetic", IEEE Tran. On Pattern Analysis and Machine Intelligence, vol.27, no.6.

[3] Plamondon, R. and Srihari, S. N., 2000, "Online and Off-line Handwriting Recognition: A Comprehensive Survey" IEEE Tran. On Pattern Analysis and Machine Intelligence, vol.22, no.1, pp 63-84 .

[4] Coetzer, J., Herbst, B.M., Du Preez, J. A., 2004, "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model" EURASIP Journal on Applied Signal Processing, 4, pp 559-571.

[5] Banshider Majhi, Santhosh Reddy,Y., Prasanna Babu, D., 2006, "Novel Features for Off-line Signature Verification" International Journal on Computers, Communications and Control, vol.1, No.1, pp.17-24.

[6] Meenakshi K. Kalera, Sargur Srihari, Aihua Xu, 2004, "Offline signature verification and identification using distance statistics" International Journal of Pattern Recognition and Artificial Intelligence Vol. 18, No. 7, pp 1339-1360.

[7] Meenakshi K. Kalera, "Offline Signature Verification and Identification using Distance Statistics" Department of Computer Science and Engineering, SUNY at Buffalo, New York, USA.

[8] Yiwei Wang & John Doherty, Robert E. Vam Dyck, "A Rotation, Scalling & Translation Resilient image watermarking algorithm using circular Gaussian Filters".

[9] A to Z Image Processing Concepts. http:/ / www.mums.ac.ir

[10] Eusuf, Md. Abu, "Differential Calculas", Part-1 & Part-2.

[11] S.E. Dreyfus, 1965, Dynamic Programming and the Calculus of Variations. Academic Press.

[12] Brault, J.J. and Plamondon, R., 1993, "Segmanting Handwritten Signatures at Their Perceptually Important Points",IEEE Trans. Pattern Analysis and Machine Intelligence, vol.15, no. 9, pp.953-957.

[13] LMunich, M.E. and Perona, P., 1999, Visual based ID verification by signature tracking. In Proc. 2nd Int. Conf. Audio and Videa Based Person Authentication.

[14] Lam, L., Suen, C.Y., 1991, A dynamic shape preserving thinning algorithm. Signal Processing 22, pp 199-208.

[15] Meng Ma, Arjan van Genderen and Peter Beukelman "Developing and Implementing Peak Detection for Real-Time Image Registration" Computer Engineering, EEMCS, TU Delft, the Netherlands, Mekelweg, The Netherlands.

[16] Jin Feng, and Huaxiang Lu, 2006, "Peak Analysis of Grayscale Image: Algorithm and Application" International Journal of Information Technology Vol. 12 No. 5.