International
Journal
Of Advanced Research in Engineering & Management (IJAREM)

A New Scheme for On-Line Signature Verification

Ms. Swati M. Patil[1], Ms. Prajakta A. Satarkar[2]
**(Department of Computer science and Engg., SVERI's College of Engg., India)*
***(Department of Computer science and Engg., SVERI's College of Engg., India)*

ABSTRACT : In this paper, we are going to propose a new technique for On-Line signature based on global n local features. In general, shape of an on-line signature is used as a single discriminating feature. Sometimes shape of signature is used alone for verification purposes and sometimes it is used in combination with some other dynamic features such as velocity, pressure and entropy. In proposed system shape of signature is examined using Edge-Detection Algorithm (EDA), pressure points are calculated using Pressure Points Allocation using Clustering (PPAC). So the overall process can be thought as the process is signature examination based on shape and pressure points in combination with entropy and velocity and it performs verification on each partition separately. Finally, the signature is classified as genuine or a forgery.
Keywords : On-Line Signature, Edge-Detection Algorithm (EDA),pressure points, Pressure Points Allocation using Clustering (PPAC)

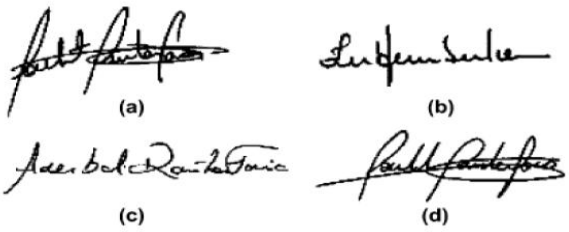
I. INTRODUCTION

1.1 Background and Motivation

Signature verification techniques utilize many different characteristics of an individual's signature in order to identify that individual. The advantages of using such an authentication techniques are
(i) Signatures are widely accepted by society as a form of identification and verification.
(ii) Information required is not sensitive.
(iii) Forging of one's signature does not mean a long-life loss of that one's identity.
The basic idea is to investigate a signature verification technique which is not costly to develop, is reliable even if the individual is under different emotions, user friendly in terms of configuration, and robust against imposters.
In signature verification application, the signatures are processed to extract features that are used for verification. There are two stages called enrollment and verification. In determining the performance of the verification system the selection of features takes main role and it is critical. The features are selected based on certain criterions. Mainly, the features have to be small enough to be stored in a smart card and do not require complex techniques. There are two types of features that validating a signature. They are static and dynamic features.
Static features are those, which are extracted from signatures that are recorded as an image whereas dynamic features are extracted from signatures that are acquired in real time. The features are of two types, function based and parameter based features. The function based features describes a signature in terms of a time-function.
Function based feature examples include position, pressure and velocity. Even though the performance of such features is accurate in verifying signatures, they are not suitable in this case due to the complexity of its matching algorithm. Hence, use of parameter based features is more appropriate.
It is important to take into account external factors when investigating a signature verification technique. Nowadays signature verification applications are used in our daily lives and will be exposed to human emotions. The system has to give reliable accuracy in verifying an individual's signature even if user is under different emotions.[1]

Types of Signature verification

Signature verification is split into two according to the available data in the input.
Offline (Static): The input of offline signature verification system is the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Some examples of offline signature shown in following figure.



Online (Dynamic): Signatures that are captured by data acquisition devices like pressure-sensitive tablets (shown in Figure 1.3) and webcam that extract dynamic features of a signature in addition to its shape (static), and can be used in real time applications like credit card transactions, protection of small personal devices (e.g. PDA), authorization of computer users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings.[1] On-Line signature is as shown in following figure.

II. PRESENT PAPERS REVIEW

Some of the recent and most relevant works are summarized below:

On-line Handwritten Signature Verification using HMM Features:
In this paper[6], Kashi proposed a method for the automatic verification of on-line handwritten signatures using both global and local features. He explained that with the addition to the global features of a local feature based on the signature likelihood obtained from Hidden Markov Models (HMM), the performance of signature verification method improved significantly. In this paper, he models the signing process with many states that constitute a Markov chain, each of them corresponding to a segment of signature. The states are not directly observable (hidden); one can only observe the signature local features here as tangent anglesThe HMM likelihood method of the signature verification performed comparable to the Euclidean distance rule for this observation vector.

Dynamic Signature Verification using Local and Global Features:

In this paper [7], Pippin proposed two verification filters, each filter employing different techniques commonly used in the literature. The first filter extracts high-level global features of a signature and compares these features with stored signature templates using KNN classification. The second filter uses velocity based stroke segmentation to encode the signature as a series of strokes and then uses dynamic time warping to find the closest distance between test and template signatures. Considering only global features of a signature has advantages that it is simple to compute and addresses privacy concerns.

New extreme points warping technique:

In this paper [8], Feng proposed a new warping technique for the functional base approach in signature verification. Dynamic time warping (DTW) is the commonly used warping technique. There are two common methodologies to verify signatures: the functional approach and the parametric approach so the functional based approach was originally used in application speech recognition and has been applied in the field of signature verification with some successful accuracy since two decades ago. The new warping technique he proposed, named as extreme points warping (EPW). It was proved that this method is adaptive in the field of signature verification than DTW in the presence of the forgeries.

Wavelet Transform Based Global Features:
In this paper a system proposed by F.A. Afsar [9], U. Farukh and M Arif. They worked in such a way that first the global features are extracted from the spatial coordinates and these features are obtained during the data acquisition stage. The method used here is one dimensional wavelet transform. Then the results are obtained using K-NN classifier and proved the accuracy of the proposed technique better. It is global feature based approach signature verification. The signature patterns are matched based on wavelet domain features that are extracted from the normalized spatial coordinates of the signatures obtained during data acquisition. The differences between the spatial coordinates of consecutive points in the signature are also subjected to both wavelet decomposition and feature extraction.

III. PROPOSED TECHNIQUE

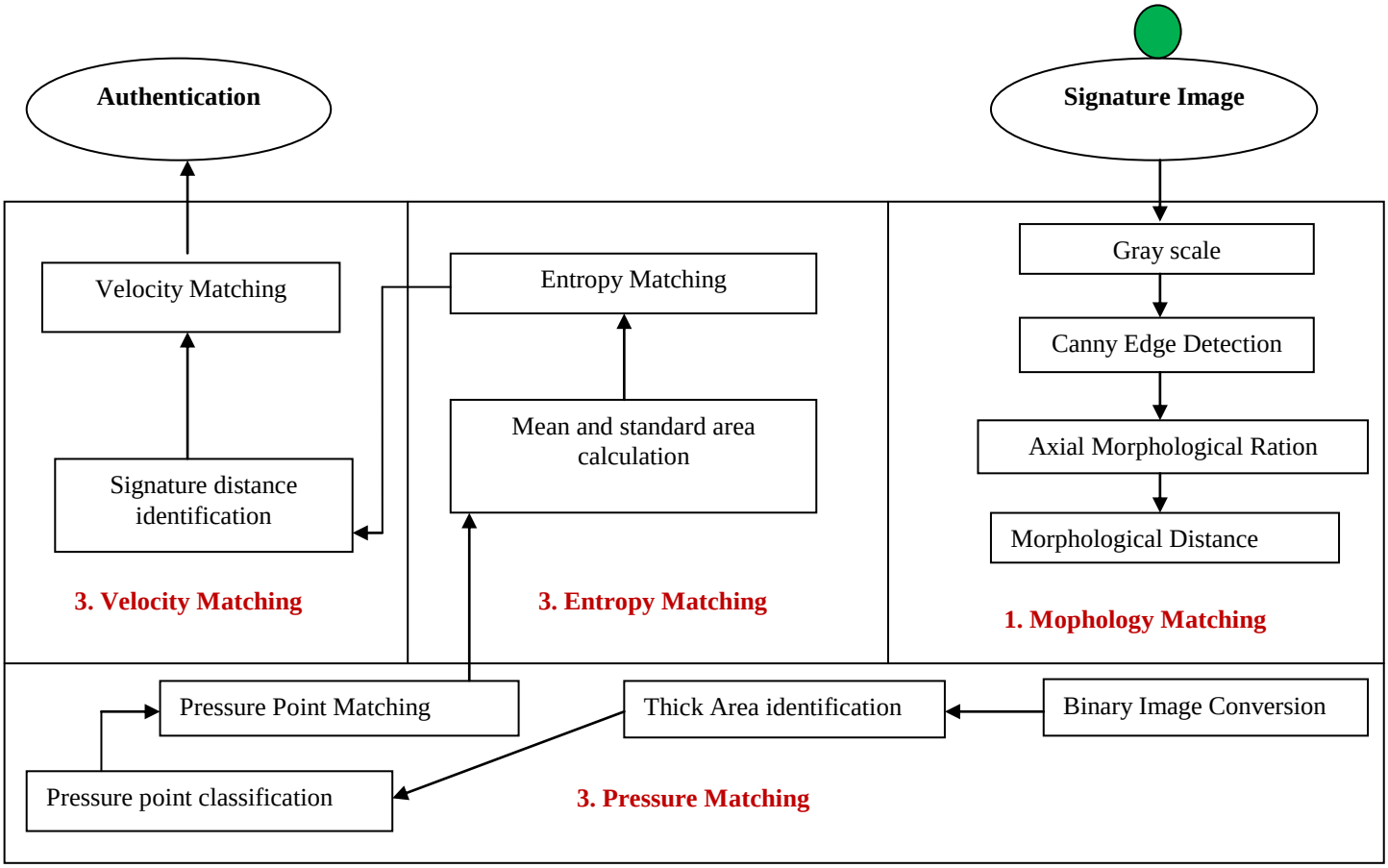
We implemented online signature verification system examines shape of signature using Edge Detection Algorithm (EDA) along with pressure points using Pressure Point allocation using pixels (PPAP) in combination with entropy and velocity features.

System Architecture:

This system has four phases as follows:

1. Distance Matching(Morphology)
2. Calculation of pressure points
3. Entropy matching
4. Velocity calculation

Overall System Architecture is as shown in figure



A. **Distance Matching**

1. This first phase of our system which consist of following steps: Take input signature (image)
2. Convert it into gray scale image (grayscale)

The grayscale conversion is implemented by grayscale conversion algorithm, which convert color image into grayscale image. Algorithm applies on original input image characterized by shadow region. In this algorithm, first calculate length (l) and width (w) of image. Get pixel value in integer format at (x,y) position of image, where x is the distance from the origin in the horizontal axis, y is the distance from the origin in the vertical axis. Convert this integer value into hexadecimal value. By doing this, we get Red(R), Green (G) and Blue (B) of that pixel. Then calculate GRAY value for that pixel by using equation (1). Apply this calculated GRAY value to each Red(R), Green (G) and Blue (B) value of that pixel i.e. R=GRAY, G=GRAY, B=GRAY. Now reset this new Red(R), Green (G) and Blue (B) to that pixel. Apply same step for pixels from 0 to width (w) and for pixel from 0 to length (l). Finally we get grayscale image.

$GRAY = (R + G + B)/3$

Figure4.1: Gray Scale Image

3. Apply Canny Edge-Detection algorithm(edgeimage)

Algorithm for Guassian Blur using in Canny Edge :

Step 0: Start
Step 1: Get Image path
Step 2: Get Length and width of the Image (L*W)
Step 3: FOR pixels from 0 to width
Step 4: FOR pixels from 0 to Length
Step 5: Get a Pixel at (x, y)
Step 6: Get the Standard Deviation of the pixel (SD)
Step 7: Calculate 1/(2 * pi *SD*SD)
Step 8: Calculate Exponent of - (x*x +y*y)/ (2*SD*SD)
Step 9: Calculate Product of step7 and Step 8 that is G
Step 10: Apply G to Pixel
Step 11: Stop

GAUSSIAN BLUR EQUATION

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

The algorithm runs in 5 separate steps:
1. Smoothing: Blurring of the image to remove noise.

- The image is smoothed by applying a Gaussian filter.

2. Finding gradients: The edges should be marked where the gradients of the image has large magnitudes.

- The Canny algorithm basically finds edges where the grayscale intensity of the image changes the most. These areas are found by determining gradients of the image.

exp(-(x * x) / (2f * sigma * sigma)

3. Non-maximum suppression: Only local maxima should be marked as edges.

- Non-maximum suppression is done to convert the "blurred" edges in the image of the gradient magnitudes to "sharp" edges.
- Basically this is done by preserving all local maxima in the gradient image and deleting everything else.

4. Double thresholding: Potential edges are determined by thresholding.

- Edge pixels stronger than the high threshold are marked as strong.
- Edge pixels weaker than the low threshold are suppressed.
- Edge pixels between the two thresholds are marked as weak.

5. Edge tracking by hysteresis: Final edges are determined by suppressing all edges that are not connected to a very certain (strong) edge.

- Strong edges are interpreted as "certain edges", and can immediately be included in the final edge image.
- Weak edges are included if and only if they are connected to strong edges.

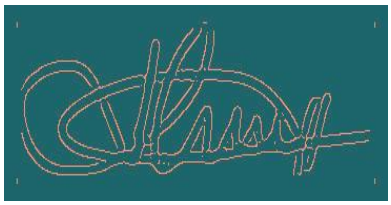


Figure4.2: Edge Image

4. Signature Morphology and morphological distance

The morphology of the any signature yields the shape and structure of the signature which eventually helps to identify the right signature. In this methodology we are considering the single axis coherent method of shape identification based on the coaxial ratio. In this process upper x axis of the signature is considered as the stagnant axis which keep recording the ratios as shown in the below algorithm.

Algorithm for Signature morphology identification

Step 0: Start
Step 1: Get Image path.
Step 2: Get Height and width of the Image (L*W).
Step 3: FOR x=0 to width.
Step 4: FOR y=0 to Height.
Step 5: Get a Pixel at (x, y) as signed integer.
Step 6: Convert pixel integer value to Hexadecimal to get R, G, and B.
Step 7: if (R!=255 and G!=255 and B!=255) (checking for signature pixel)
Step 8: Get the Y value for the pixel
Step 9: Then ratio $R_{t=}$ Y/Height
Step 10: Add R_t into an array called RA
Step11: End of inner for
Step 12: End of outer for
Step 13 : Stop

Here in the above algorithm Array called RA indicates the morphological array which induces the shape of the signature image with correlation of x Axis.

The distance between the two signatures can be identified as shown in the below algorithm

Algorithm for morphological distance matching

Input R_i and R_d as two distance arrays of input signature and every dataset signature

Step 0 : Start
Step 1: Initialize sum S=0
Step 1: for i=0 to length of R_i and R_d
Step 2: get x and y as elements of R_i and Rd respectively
Step 3: d=x-y
Step 5: S=S+d
Step 6: End of for
Step 7: distance=S/ length of R_i
Step 8: Stop

Then the smallest distance with the signature is considered as the matched one.

4.3. Pressure Matching

In this phase we calculating pressure points of input image with the help of pressure point allocation using pixel(PPAP) [9]. Actual implementation of this phase is divided into following steps:

4.3.1. Binary Image conversion

In this step signature image is converted into binary image based on the black and white component of the image pixels. By doing this we can get the complete image that contains only two colored pixels like black and white. By doing this our system efficiently removes all other colored pixels which can be a barrier to identify the pressure points in the image. Below algorithm shows clearly the steps of binary conversion .

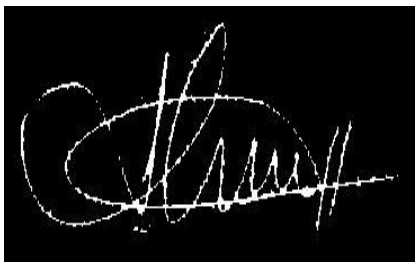


Figure 4-5: Binary Image

1.3.2. Thick Area identification:

After Binary image we have to perform thick area detection using clustering based clusters we are going to identify thick area if signature.

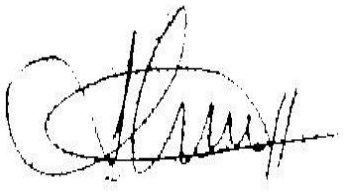


Figure 4-3: AreaSegmented Image

4.3.3. Pressure point classification:

Detected thick area is now considered as pressure points again we are applying here clustering using nearest four pixel as one pressure point**.**

Figure 4-6: Pressure Points

4.3 Entropy matching

After validation of pressure calculation phase we are considering entropy of image based RGB factors.

4.4 Velocity calculation

Velocity of image is calculated as:
Total length of signature(max X-min X)/ average time.
Velocity match(InputImage Velocity, DataSetImageVelocity)

IV. RESULT ANALYSIS

To measure this precision and recall are considering as the best measuring techniques. So precision can be defined as the ratio of the number of relevant signatures authenticated to the total number of irrelevant and relevant signatures are authenticated. It is usually expressed as a percentage. This gives the information about the relative effectiveness of the system. Whereas Recall is the ratios of the number of relevant signatures are authenticated to the total numbers of relevant signatures are not authenticated. It is usually expressed as a percentage. This gives the information about the absolute accuracy of the system.

The advantage of having the two for measures like precision and recall is that one is more important than the other in many circumstances.

For more clarity let we assign

- A = The number of relevant signatures are authenticated,
- B = The number of relevant signatures are not authenticated and
- C = The number of irrelevant signatures are authenticated.

So, Precision = (A/ (A+ C))*100

And Recall = (A/ (A+ B))*100

To measure the performance of the model, system is set to authenticate signature images of 10 input images at each run. The performance is shown in the below figure.

Figure 4.1: Average precision of the proposed approach

In Figure 4.1, we observe that the tendency of average precision for the authenticating signature images are high compared to other systems.

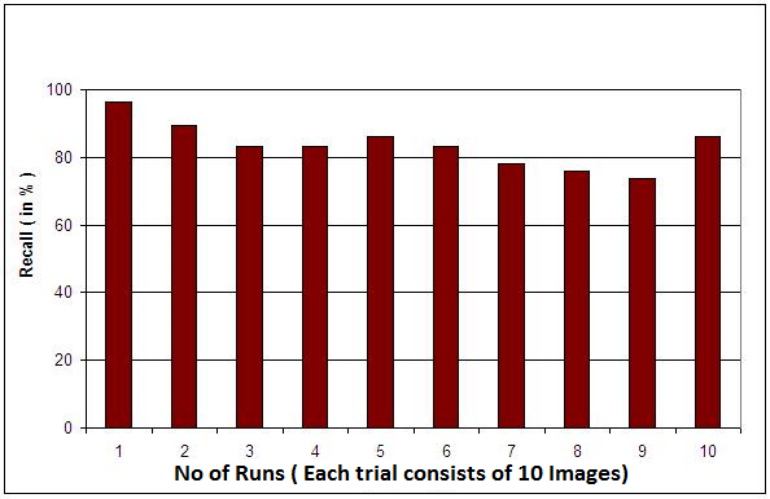


Figure 4.2: Average Recall of the proposed approach

In Figure 4-2, we observe that the tendency of average Recall for authenticating signature images are high compared to other system. So this shows that our proposed system is achieving high accuracy than any other method.

V. CONCLUSION

In this paper, We analysed online signature verification by global features pressure with entropy and velocity. By employing dynamic features (velocity and pressure) and extracting signature shape of a given signer, it is made impossible for a forger to maintain shape within a certain velocity and pressure partition at a given time. The data base used for the verification was not large. Thus, this technique should be verified with large data base. Only the local features were considered for verification and evaluated independently.

REFERENCES

Journal Papers:

[1]. Kiran Kumar "A New On-Line Signature Verification Algorithm",Telematics and Signal Processing , 209EC1103,Rourkela ,2011.

[2]. Prashanth C R ,Department of ECE, Vemana Institute of Technology Bangalore, India "DWT based Off-line Signature Verification using Angular Features", International Journal of Computer Applications (0975 – 8887) Volume 52– No.15, August 2012.

[3]. Mohammad A. U. Khan, Velocity-Image Model for OnlineSignature Verification, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 11, NOVEMBER 2006.

[4]. Daigo Muramatsu, Effectiveness of Pen Pressure, Azimuth, andAltitude Features for Online Signature Verification, Seikei University,3-3-1 Kichijoji-kitamachi, Musashino-shi, Tokyo 180-8633.

[5]. Mohammad M. Shafiei, Hamid R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models," Seventh International Conference on Document Analysis and Recognition (ICDAR'03), vol. 1, pp. 443, 2003.

[6]. R. S. Kashi , J. Hu & W. L. Nelson, "On-line Handwritten Signature Verification using Hidden Markov Model Features", Fourth International Conference Document Analysis and Recognition (ICDAR'97), pp. 253 – 257, 1997.

[7]. Charles E. Pippin, "Dynamic Signature Verification using Local and Global Features", Georgia Institute of Technology, July 2004.

[8]. Hao Feng and Chan Choong Wah, "Online Signature Verification Using New Extreme Points Warping Technique", Pattern Recognition Letters, vol. 24, pp. 2943-2951, Dec. 2003.

[9]. F.A. Afsar, M. Arif and U. Farrukh, "Wavelet Transform Based Global Features for Online Signature Recognition", Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[10]. Liang Wan, Bin Wan, Zhou-Chen Lin "On-Line Signature Verification with Two-Stage Statistical Models", Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 – 286, 2005.

[11]. Cman F. Lam, David Kamins and Kuno Zimerann, "Signature Recognition through Spectral Analysis", Pattern Recognition, vol. 22, pp.39-44, Jan.1989.

[12]. Anil K. Jain, Friederike D. Griess, Scott D. Connell," On-line signature verification", Pattern Recognition ,vol .35 2963 – 2972,2002.